Submission of the Citizen Lab at the Munk School of Global Affairs & Public Policy, University of Toronto, to the Committee on Enforced Disappearances and the Working Group on Enforced or Involuntary Disappearances

January 31, 2026

Report authors:

Siena Anstis
Tristan Surman
Noura Aljizawi
Dr. Marcus Michaelsen
Dr. Ron Deibert

For all inquiries regarding this submission, please contact:

Dr. Ronald J. Deibert, Director, The Citizen Lab, Munk School of Global Affairs, Professor of Political Science, University of Toronto, r.deibert@utoronto.ca

Table of Contents

Introduction

The Citizen Lab welcomes the opportunity to submit to the Committee on Enforced Disappearances ("the Committee") and the UN Working Group on Enforced and Involuntary Disappearances ("the Working Group"). It is timely that the Committee and the Working Group engage with the issue of transnational repression which poses a threat not only to the human rights of those targeted but also to the rule of law within the countries where they reside. Perpetrating states are, in part, able to carry out acts of transnational repression due to a lack of public awareness and the absence of sustained pressure on host state governments to respond through formal legal mechanisms. Where transnational repression is primarily framed as an affront to state sovereignty and national security or managed through diplomatic backchannels, victims of these practices are routinely denied access to effective remedy. To address the global proliferation of these practices, the human rights violations they entail, and the obligation of host states to prevent and to respond to them, it is critical that bodies like the Committee and the Working Group systematically identify and document acts of transnational repression, characterize them explicitly as human rights violations, and assess the responsibility of state actors involved.

Highlighting the digital tactics of transnational repression is an essential component of broader efforts to address and prevent such practices. Digital transnational repression

functions as a precursor to, and enabler of, enforced disappearances and other serious acts of transnational repression, including extraterritorial killings or extraterritorial abductions. Surveillance of a target's daily habits and movement patterns – carried out through spyware or other digital methods that facilitate location tracking – underpins the execution of an enforced disappearance in another state.

In this submission, we thus build on our prior submission to the Working Group on the role of spyware in enforced disappearances.[1] We continue to highlight the role of digital technologies – in particular, spyware and other location-tracking technologies that exploit advertising data and vulnerabilities in our global telecommunications infrastructure – in facilitating transnational enforced disappearances.

About the Citizen Lab

Founded in 2001 by Professor Ronald J. Deibert, the Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

The Citizen Lab uses a "mixed methods" approach to research combining methods from political science, law, computer science, and area studies. Our research includes investigating digital espionage against civil society; documenting Internet filtering and other technologies and practices that impact freedom of expression online; analyzing privacy, security, and information controls of popular applications; and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

[1] Siena Anstis, Dr. Ronald J. Deibert, Émilie LaFlèche, and Jon Penney (2022), "Submission of the Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto) to the United Nations Working Group on Enforced or Involuntary Disappearances," *The Citizen Lab* (June 18, 2022) <https://citizenlab.ca/wp-content/uploads/2022/07/Submission-of-the-Citizen-Lab-Munk-School-of-Global-Affairs-University-of-Toronto-to-the-United-Nations-Working-Group-on-Enforced-or-Involuntary-Disappearances.pdf>.

How Digital Transnational Repression Facilitates Transnational Enforced Disappearances

What is Digital Transnational Repression?

Transnational repression is a term used to describe how states reach across borders using different methods – such as enforced disappearances, killings, abductions, extraditions, and harassment or other physical attacks – to silence dissent and/or impair the human rights of diaspora and exiled communities.[2] Digital technologies offer governments that perpetrate acts of transnational repression a low-cost means to expand the scope and scale of their repressive activities. Digital transnational repression is a specific form of transnational repression that employs digital technologies to surveil, intimidate, and silence individuals living in exile or in the diaspora.[3] It can feed into acts of physical transnational repression. Digital transnational repression includes the following methods:

- **Surveillance:** Monitoring online communications to gather, analyze, and exploit information on the activities, daily habits, location, and social networks of targets, with the aim to expose country of origin contacts or prepare further attacks such as a transnational enforced disappearance.
- **Interception:** Hacking of electronic devices, email, and social media accounts to access private information, communications, and contacts. These forms of targeted, invasive surveillance can rely on phishing attacks, physical access to a device, or the remote use of spyware.
- **Intimidation and stigmatization:** Using private, false, and distorted information, as well as online harassment and online threats, to silence and discredit targets.
- **Disruption:** Curtailing expression on blogs, news/organizations' websites, and social media profiles through distributed denial-of-service (DDoS) attacks, false reports, spam comments, content filtering, and information manipulation.

Digital threats and attacks that form part of a practice of digital transnational repression can set the stage for an escalation into physical threats and attacks, including transnational

[2] Noura Al-Jizawi, Siena Anstis, Sophie Barnett, Sharly Chan, Niamh Leonard, Adam Senft, and Ron Deibert (2022), "Psychological and Emotional War: Digital Transnational Repression in Canada," *The Citizen Lab* (March 1, 2022) <https://citizenlab.ca/wp-content/uploads/2022/03/Report151-dtr_022822.pdf>.
[3] Noura Aljizawi, Siena Anstis, Marcus Michaelsen, Veronica Arroyo, Shaila Baran, Maria Bikbulatova, Gözde Böcü, Camila Franco, Arzu Geybulla, Muetter Iliqud, Nicola Lawford, Émilie LaFlèche, Gabby Lim, Levi Meletti, Maryam Mirza, Zoe Panday, Claire Posno, Zoë Reichert, Berhan Taye, and Angela Yang (2024), "No Escape: The Weaponization of Gender for the Purposes of Digital Transnational Repression," *The Citizen Lab* (December 2, 2024) <https://citizenlab.ca/wp-content/uploads/2024/12/Report180-noescape112924.pdf>.

enforced disappearances. As such, digital transnational repression is considered a core element of all forms of transnational repression. Digital tools enable authoritarian governments to easily instill fear and uncertainty among exiled human rights defenders and members of civil society more broadly, undermine the social relationships within exile and diaspora communities and their countries of origin, and foster self-censorship and withdrawal from activism.[4] Digital tools also allow governments to track the location of a target outside the country's borders, and to map their network of contacts.

Examples of Digital Transnational Repression in the Context of Transnational Enforced Disappearances

Mercenary Spyware

As we described in our prior submission to the Working Group, spyware is a form of malicious software that allows an operator to gain remote access to (or "hack") a device in order to extract, modify, or share its contents.[5] Devices can be infected with spyware through different mechanisms such as (a) exploit links that require the target to click a link or open a document to begin the infection process; (b) zero-click exploits that require no interaction from the target for the spyware to be installed; or (c) through manual installation in cases where the state operator has physical access to the phone, such as a temporary confiscation of the device.[6]

Depending on the sophistication of the spyware, an infection may give the perpetrator full access to a target's device. For example, infection with Pegasus, a spyware developed by

[4] Noura Aljizawi, Siena Anstis, Marcus Michaelsen, Veronica Arroyo, Shaila Baran, Maria Bikbulatova, Gözde Böcü, Camila Franco, Arzu Geybulla, Muetter Iliqud, Nicola Lawford, Émilie LaFlèche, Gabby Lim, Levi Meletti, Maryam Mirza, Zoe Panday, Claire Posno, Zoë Reichert, Berhan Taye, and Angela Yang (2024), "No Escape: The Weaponization of Gender for the Purposes of Digital Transnational Repression," *The Citizen Lab* (December 2, 2024) <https://citizenlab.ca/wp-content/uploads/2024/12/Report180-noescape112924.pdf>.

[5] Siena Anstis, Dr. Ronald J. Deibert, Émilie LaFlèche, and Jon Penney (2022), "Submission of the Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto) to the United Nations Working Group on Enforced or Involuntary Disappearances," *The Citizen Lab* (June 18, 2022) <https://citizenlab.ca/wp-content/uploads/2022/07/Submission-of-the-Citizen-Lab-Munk-School-of-Global-Affairs-University-of-Toronto-to-the-United-Nations-Working-Group-on-Enforced-or-Involuntary-Disappearances.pdf>.

[6] Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert (2018), "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," *The Citizen Lab* (September 18, 2018) at 7 <https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>.

Israeli surveillance company NSO Group, can give state actors access to all of the target phone's contents and passwords, as well as the ability to download files, listen to telephone calls, track the target's location, and remotely turn on the microphone and camera.[7] These infections can even successfully eavesdrop on encrypted calls and messages.[8]
As described in our earlier submission, spyware is used by states in a manner that violates a range of human rights.[9] More specifically, we have identified multiple cases where spyware was used by states in the context of enforced disappearances (or advocacy efforts by relatives of a victim around an enforced disappearance) with a transnational element to the targeting.

Spyware has been linked to the enforced disappearance of Loujain Alhathloul, a human rights defender and prominent women's rights activist from Saudi Arabia.[10] In 2018, Alhathloul was arbitrarily detained in the United Arab Emirates and forcibly rendered to Saudi Arabia, where she was placed under a travel ban.[11] Upon arrival in Saudi Arabia she was subject to multiple detentions – eventually being arrested in her home by Saudi officers, imprisoned, interrogated, tortured, and threatened with rape and murder.[12] While she was being tortured, details of her private communications were mentioned and later cited in court documents.[13] Amongst other evidence, this prompted Alhathloul to file a civil action in 2021 against the Emirati cyber-surveillance company DarkMatter Group "for illegally hacking her iPhone to secretly track her communications and whereabouts."[14] The suit alleges that DarkMatter

[7] Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert (2018), "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," *The Citizen Lab* (September 18, 2018) at 7 <https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>.
[8] The Citizen Lab (2022), "Would You Click?" *The Citizen Lab* (April 18, 2022) <https://catalonia.citizenlab.ca/>.
[9] Siena Anstis, Dr. Ronald J. Deibert, Émilie LaFlèche, and Jon Penney (2022), "Submission of the Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto) to the United Nations Working Group on Enforced or Involuntary Disappearances," *The Citizen Lab* (June 18, 2022) <https://citizenlab.ca/wp-content/uploads/2022/07/Submission-of-the-Citizen-Lab-Munk-School-of-Global-Affairs-University-of-Toronto-to-the-United-Nations-Working-Group-on-Enforced-or-Involuntary-Disappearances.pdf>.
[10] Joel Schectman and Christopher Bing (2022), "Insight: How A Saudi Woman's Iphone Revealed Hacking Around The World," *Reuters* (February 17, 2022) <https://www.reuters.com/technology/how-saudi-womans-iphone-revealed-hacking-around-world-2022-02-17/>.
[11] EFF (2021), "AlHathloul v. DarkMatter Group – Complaint," *EFF* (December 9, 2021) at para 9 <https://www.eff.org/document/alhathloul-v-darkmatter-group-complaint>.
[12] EFF (2021), "AlHathloul v. DarkMatter Group – Complaint," *EFF* (December 9, 2021) at para 27; 116 - 130 <https://www.eff.org/document/alhathloul-v-darkmatter-group-complaint>.
[13] EFF (2021), "AlHathloul v. DarkMatter Group – Complaint," *EFF* (December 9, 2021) at para 27, 30 <https://www.eff.org/document/alhathloul-v-darkmatter-group-complaint>.
[14] EFF (2021), "Saudi Human Rights Activist, Represented by EFF, Sues Spyware Maker DarkMatter for Violating U.S. Anti-Hacking and International Human Rights Law," *EFF* (December 9, 2021) <https://www.eff.org/press/releases/saudi-human-rights-activist-represented-eff-sues-spyware-maker-darkmatter-violating>.

surveilled her and shared the resulting information with Emirati security services in support of their efforts to detain her and ultimately transfer her to Saudi Arabia.[15] These surveillance tactics, the suit alleges, fit within a broader Emirati "campaign of targeting and persecuting perceived dissidents" through "advanced cyber-surveillance programs" enabled by commercial spyware.[16] In 2022, the Citizen Lab confirmed that a powerful "zero-click" form of spyware had been installed on Althathloul's phone in a way that did not require her to click on any link or download any file.[17]

Spyware was also implicated in the killing of Jamal Khashoggi, a journalist and critic of the Saudi government who was killed by Saudi authorities in the Saudi consulate in Istanbul, Turkey on October 2, 2018. Forensic research shows that people close to Khashoggi had their devices hacked or targeted with Pegasus spyware before and after his murder ("relational targeting", i.e., the targeting of friends or family of the ultimate target, is an effective means by which to track a target without directly infecting their device). Khashoggi's wife, Hanan Elatr Khashoggi, had her phone infected with Pegasus spyware before the killing, between November 2017 and April 2018.[18] She believes that such surveillance may have made it easier for Saudi officials to track Khashoggi.[19] Khashoggi's fiancée, Hatice Cengiz, was targeted with Pegasus spyware four days after his murder.[20] Omar Abdulaziz, who was a close associate of Khashoggi, also had his phone infected with Pegasus spyware prior to Khashoggi's assassination in 2018.[21] The surveillance may have informed Saudi officials of "sensitive plans

---

[15] EFF (2021), "AlHathloul v. DarkMatter Group – Complaint," *EFF* (December 9, 2021) at para 6 <https://www.eff.org/document/alhathloul-v-darkmatter-group-complaint>.
[16] EFF (2021), "AlHathloul v. DarkMatter Group – Complaint," *EFF* (December 9, 2021) at para 50 <https://www.eff.org/document/alhathloul-v-darkmatter-group-complaint>.
[17] Joel Schectman and Christopher Bing (2022), "Insight: How A Saudi Woman's Iphone Revealed Hacking Around The World," *Reuters* (February 17, 2022) <https://www.reuters.com/technology/how-saudi-womans-iphone-revealed-hacking-around-world-2022-02-17/>.
[18] Philip Bennett (2021), "Pegasus Spyware Placed on Phone of Jamal Khashoggi's Wife Before his Murder, Washington Post Reports," *PBS Frontline* (21 December 2021) <https://www.pbs.org/wgbh/frontline/article/pegasus-spyware-jamal-khashoggi-wife-phone-washington-post/>.
[19] Philip Bennett (2021), "Pegasus Spyware Placed on Phone of Jamal Khashoggi's Wife Before his Murder, Washington Post Reports," *PBS Frontline* (21 December 2021) <https://www.pbs.org/wgbh/frontline/article/pegasus-spyware-jamal-khashoggi-wife-phone-washington-post/>.
[20] Dana Priest, Souad Mekhennet, and Arthur Bouvart (2018), "Jamal Khashoggi's Wife Targeted with Spyware Before his Death," *The Washington Post* (18 July 2018) <https://www.washingtonpost.com/investigations/interactive/2021/jamal-khashoggi-wife-fiancee-cellphone-hack/>.
[21] Bill Marczak, John Scott-Railton, Adam Senft, Bahr Abdul Razzak, and Ron Deibert (2018), "The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil," *The Citizen Lab* (October 1, 2018) <https://tspace.library.utoronto.ca/bitstream/1807/95329/1/Report%23115--Kingdom%20Came.pdf>.

he had been developing with Khashoggi" in their activism against the Saudi government.[22] Others around Khashoggi were also suspected to have been targeted with spyware.[23]

Beyond its use to target Saudi dissidents abroad, spyware played an important role in the case of Paul Rusesabagina, a long-time critic of Kagame's government in Rwanda.[24] In August 2020, Rusesabagina was forcibly disappeared on a layover in Dubai on his way to Burundi.[25] A few days later, he was imprisoned in Rwanda for purportedly "financing terrorist activities."[26] His daughter, Carine Kanimba, claimed that the charges against her father were fraudulent and politically motivated, launching a campaign advocating for his release.[27] Amnesty International discovered that Kanimba's phone had likely been infected with Pegasus spyware starting in January 2021.[28] The Rwandan government had been listening to her phone calls with lawyers, members of the Belgian, British, and the European Parliament, as well as United

[22] Ayman M. Mohyeldin (2019), "No One is Safe: How Saudi Arabia Makes Dissidents Disappear," *Vanity Fair* (July 29, 2019) <https://www.vanityfair.com/news/2019/07/how-saudi-arabia-makes-dissidents-disappear>.
[23] Haaretz (2021), "Khashoggi's Fiancee, Son Targeted by NSO Tech, Investigation Reveals," *Haaretz* (18 July 2021) <https://www.haaretz.com/israel-news/tech-news/2021-07-18/ty-article/.premium/khashoggis-fiancee-son-targeted-by-nso-tech-investigation-reveals/0000017f-dc92-db5a-a57f-dcfa206c0000>; BBC (2021), "Pegasus: Who are the alleged victims of spyware targeting?" *BBC* (22 July 2021) <https://www.bbc.com/news/world-57891506>; Dana Priest, Souad Mekhennet and Arthur Bouvart (2021), "Jamal Khashoggi's Wife Targeted With Spyware Before His Death," *The Washington Post* (18 July 2021) <https://www.washingtonpost.com/investigations/interactive/2021/jamal-khashoggi-wife-fiancee-cellphone-hack/>.
[24] Stephanie Kirchgaessner (2021), "Hotel Rwanda Activist's Daughter Placed Under Pegasus Surveillance," *The Guardian* (19 July 2021) <https://www.theguardian.com/news/2021/jul/19/hotel-rwanda-activist-daughter-pegasus-surveillance>.
[25] OCCRP (2021), "Israeli Spy Tech Used Against Daughter of Man Who Inspired 'Hotel Rwanda,'" *OCCRP* (19 July 2021) <https://www.occrp.org/en/the-pegasus-project/israeli-spy-tech-used-against-daughter-of-man-who-inspired-hotel-rwanda>.
[26] OCCRP (2021), "Israeli Spy Tech Used Against Daughter of Man Who Inspired 'Hotel Rwanda,'" *OCCRP* (19 July 2021) <https://www.occrp.org/en/the-pegasus-project/israeli-spy-tech-used-against-daughter-of-man-who-inspired-hotel-rwanda>.
[27] Stephanie Kirchgaessner (2021), "Hotel Rwanda Activist's Daughter Placed Under Pegasus Surveillance," *The Guardian* (19 July 2021) <https://www.theguardian.com/news/2021/jul/19/hotel-rwanda-activist-daughter-pegasus-surveillance>; Al Jazeera, "World Reaction to 'Hotel Rwanda' Hero's Prison Sentence," *Al Jazeera* (20 September 2021) <https://www.aljazeera.com/news/2021/9/20/world-reaction-hotel-rwanda-star-jailed>.
[28] Stephanie Kirchgaessner (2021), "Hotel Rwanda Activist's Daughter Placed Under Pegasus Surveillance," *The Guardian* (19 July 2021) <www.theguardian.com/news/2021/jul/19/hotel-rwanda-activist-daughter-pegasus-surveillance>.

States officials.[29] Rwandan government officials also revealed that they knew about legal plans discussed privately between Rusesabagina's family and their lawyers.[30] In addition to undermining efforts to free Rusesabagina, Kanimba also argues that the spyware was being used as "an intimidation tool."[31] This is consistent with a broader practice of states using surveillance and other intimidation tactics against family members "because of their ease for the origin state and degree to which they can affect the target."[32]

The alleged use of spyware by the Rwandan government has not been limited to Rusesabagina. In 2019, a Belgium-based Rwandan activist was forcibly disappeared during a trip to Uganda.[33] David Batenga, one of the activist's associates who had helped arrange the trip, worries that information stolen from his phone using Pegasus spyware may have been used to effect the disappearance.[34] Although a forensic analysis on Batenga's device was not possible in this case, it nonetheless evokes the practice of "relational targeting," the use of spyware against close associates or family members to monitor communications and compile critical information about the targets and individuals in their network.[35] Concerns about this practice were also raised by Placide Kayumba, an exiled Belgium-based Rwandan political activist and the vice president of the FDU-Inkingi party, who suggested that the murder of two

[29] Stephanie Kirchgaessner (2021), "Hotel Rwanda Activist's Daughter Placed Under Pegasus Surveillance," *The Guardian* (19 July 2021) <www.theguardian.com/news/2021/jul/19/hotel-rwanda-activist-daughter-pegasus-surveillance>; OCCRP (2021), "Israeli Spy Tech Used Against Daughter of Man Who Inspired 'Hotel Rwanda'," *OCCRP* (19 July 2021) <https://www.occrp.org/en/the-pegasus-project/israeli-spy-tech-used-against-daughter-of-man-who-inspired-hotel-rwanda>.

[30] OCCRP (2021), "Israeli Spy Tech Used Against Daughter of Man Who Inspired 'Hotel Rwanda'," *OCCRP* (19 July 2021) <https://www.occrp.org/en/the-pegasus-project/israeli-spy-tech-used-against-daughter-of-man-who-inspired-hotel-rwanda>.

[31] OCCRP (2021), "Israeli Spy Tech Used Against Daughter of Man Who Inspired 'Hotel Rwanda'," *OCCRP* (19 July 2021) <https://www.occrp.org/en/the-pegasus-project/israeli-spy-tech-used-against-daughter-of-man-who-inspired-hotel-rwanda>.

[32] Nate Schenkkan and Isabel Linzer (2021), "Out of Sight, Not Out of Reach," *Freedom House* (February 2021) <https://freedomhouse.org/sites/default/files/2021-02/Complete_FH_TransnationalRepressionReport2021_rev020221.pdf>.

[33] Mehul Srivastava and Tom Wilson (2019), "Inside the WhatsApp hack: how an Israeli technology was used to spy," *Financial Times* (October 29, 2019) <https://www.ft.com/content/d9127eae-f99d-11e9-98fd-4d6c20050229>

[34] Mehul Srivastava and Tom Wilson (2019), "Inside the WhatsApp hack: how an Israeli technology was used to spy," *Financial Times* (October 29, 2019) <https://www.ft.com/content/d9127eae-f99d-11e9-98fd-4d6c20050229>

[35] John Scott-Railton, Elies Campo, Bill Marczak, Bahr Abdul Razzak, Siena Anstis, Gözde Böcü, Salvatore Solimano, and Ron Deibert (2022), "CatalanGate: Extensive Mercenary Spyware Operation Against Catalans Using Pegasus and Candiru," *The Citizen Lab* (April 18, 2022) <https://citizenlab.ca/research/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/>.

party members in Rwanda in 2019 may have been linked to the targeting of his device with Pegasus spyware.[36]

Further, our prior submission, as well as recent reports from the Citizen Lab and others, have revealed the systematic use of spyware against individuals involved in the investigation of enforced disappearances in Mexico.[37] This includes the surveillance of lawyers representing the families of 43 students from Ayotzinapa who were forcibly disappeared in September 2014,[38] the head of the government commission looking into the case,[39] and a researcher for the government commission on crimes (including enforced disappearances) committed during the internal conflict known as the "Dirty War".[40] Furthermore, spyware was used to target a group of international experts supporting the investigation into the Ayotzinapa case, a fact recently confirmed by former high-ranking Mexican officials.[41]

These cases illustrate how the use of spyware to conduct cross-border surveillance of dissidents, human rights defenders, journalists, and other members of civil society in exile is directly linked to the enforced disappearances of those under surveillance, as well as individuals within their professional and personal networks. Malign state actors' unconstrained ability to purchase and use these tools is at the heart of current tactics of digital transnational repression, which can lead to gross human rights violations including enforced disappearances.

---

[36] Mehul Srivastava and Tom Wilson (2019), "Inside the WhatsApp hack: how an Israeli technology was used to spy," *Financial Times* (October 29, 2019) <https://www.ft.com/content/d9127eae-f99d-11e9-98fd-4d6c20050229>

[37] Bill Marczak, John Scott-Railton, Bahr Abdul Razzak, and Ron Deibert (2023), "Triple Threat NSO Group's Pegasus Spyware Returns in 2022 with a Trio of iOS 15 and iOS 16 Zero-Click Exploit Chains," *The Citizen Lab* (April 18, 2023) <https://citizenlab.ca/research/nso-groups-pegasus-spyware-returns-in-2022/>

[38] John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert (2017), "Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware," *The Citizen Lab* (June 19, 2017) <*https://citizenlab.ca/research/reckless-exploit-mexico-nso/*>

[39] Natalie Kitroeff and Ronen Bergman (2023), "He Was Investigating Mexico's Military. Then the Spying Began," *The New York Times* (May 22, 2023) <https://www.nytimes.com/2023/05/22/world/americas/mexico-spying-pegasus-israel.html>

[40] Oscar Lopez and Mary Beth Sheridan, (2023). "He's leading Mexico's probe of the Dirty War. Who's spying on him?" *The Washington Post* (June 3, 2023) <https://www.washingtonpost.com/world/2023/06/03/mexico-pegasus-dirty-war-lopez-obrador/>

[41] John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert (2017), "Reckless III: Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware," *The Citizen Lab* (July 10, 2017) <https://citizenlab.ca/research/mexico-disappearances-nso/>; R3D (2024), "Tomás Zerón admite que el GIEI fue espiado con Pegasus y que el Ejército y CISEN también lo tenían," R3D (October 23, 2024) <https://r3d.mx/2024/10/23/tomas-zeron-admite-que-el-giei-fue-espiado-con-pegasus-y-que-el-ejercito-y-cisen-tambien-lo-tenian/>

Geolocation Tracking Using Telecommunications Vulnerabilities

In the past few years, we have also seen the expansion of cross-border surveillance through the exploitation of vulnerabilities in global telecommunications networks. This surveillance strategy has proven a powerful tool for digital transnational repression, providing states with accessible and difficult-to-trace means of tracking targets in foreign jurisdictions – clearly raising the threat of transnational enforced disappearances.

This strategy allows state operators — such as intelligence agencies — to undertake active and passive surveillance of targets in foreign jurisdictions by generating fake requests for cellphone location data from local telecommunications providers.[42] This method involves exploiting a vulnerability in the Signaling System 7 (SS7) – a protocol suite which facilitates the routing of cellphone data and phone calls between phone networks.[43] This protocol suite is particularly useful in allowing "roaming," facilitating the forwarding of communications from a subscriber's 'home network' to a 'visited network' in the country they are visiting.[44] The challenge arises from the fact that SS7 does not include authentication or access controls, meaning that any attacker that interconnects with the SS7 network (for example, by purchasing or 'leasing' SS7 access[45] or running a fake phone company[46]) can send commands to a subscriber's home network falsely indicating that the subscriber is roaming.[47] These

[42] Gary Miller and Christopher Parsons (2023), "Finding You: The Network Effect of Telecommunications Vulnerabilities for Location Disclosure," *Citizen Lab* (October 26, 2023) <https://citizenlab.ca/2023/10/finding-you-teleco-vulnerabilities-for-location-disclosure/#conclusion>.
[43] Gabriel Geiger, Crofton Black, Riccardo Coluccini, Bashar Deeb, et. al. (2025), "How First Wap Tracks Phones Around the World," *Lighthouse Reports* (October 14, 2025) <https://www.lighthousereports.com/methodology/surveillance-secrets-explainer/>.
[44] Bill Marczak, John Scott-Railton, Siddharth Prakash Rao, Siena Anstis, and Ron Deibert (2020), "Running in Circles: Uncovering the Clients of Cyberespionage Firms Circles," *Citizen Lab* (December 1, 2020) <https://utoronto.scholaris.ca/server/api/core/bitstreams/82de8ca4-5759-4d54-8c9b-7270144c8950/content>
[45] Russell Brandom (2017), "For $500, this site promises the power to track a phone and intercept its texts: Paid access to a deeply insecure phone network," *The Verge* (June 13, 2017) <https://www.theverge.com/2017/6/13/15794292/ss7-hack-dark-web-tap-phone-texts-cyber-crime>; Crofton Black, Stephanie Kirchgaessner and Dan Sabbagh (2020), "Israeli spy firm suspected of accessing global telecoms via Channel Islands," *The Guardian* (December 16, 2020) <https://www.theguardian.com/world/2020/dec/16/israeli-spy-firm-suspected-accessing-global-telecoms-channel-islands>.
[46] Intelligence Online (2015), "'Circles' 'mobile phone' company intercepts 3G," *Intelligence Online* <https://www.intelligenceonline.com/europe-russia/2015/12/02/circles---mobile-phone--company-intercepts-3g,108114286-art> (February 12, 2015).
[47] Bill Marczak, John Scott-Railton, Siddharth Prakash Rao, Siena Anstis, and Ron Deibert (2020), "Running in Circles: Uncovering the Clients of Cyberespionage Firms Circles," *Citizen Lab* (December 1, 2020) <https://utoronto.scholaris.ca/server/api/core/bitstreams/82de8ca4-5759-4d54-8c9b-7270144c8950/content>

commands allow the government operator to then track the victim's location and intercept voice calls and SMS text messages.[48]

There is strong evidence to suggest that states have exploited SS7 vulnerabilities to surveil dissidents in foreign jurisdictions. Reporting from *The Guardian*, for example, alleged that Saudi Arabia exploited SS7 to track the movements of individual subscribers to Saudi telecommunications providers who were travelling in the United States.[49] Given the above-noted history of using digital surveillance to effect enforced disappearances of activists and dissidents, Saudi Arabia's ability to use telecommunications network-based geolocation surveillance is concerning.

Beyond Saudi Arabia's tracking activities in the United States, a recent investigation by Lighthouse Reports, a not-for-profit investigative journalism group, has suggested a connection between the exploitation of SS7 networks and the assassination of Rwandan opposition leader Patrick Karegeya in Johannesburg.[50] By digging into an archive of data linked to the surveillance software Altamides – which itself was built on the exploitation of SS7 vulnerabilities – the reporting revealed that Karegeya's associates were surveilled using the software in the lead-up to his 2013 killing.[51] Beyond Karegeya's associates, the reporting showed widespread use of Altamides by private and state actors for the purposes of cross-border surveillance.[52] Such cases demonstrate a proliferating global practice of exploiting SS7 vulnerabilities to launch geolocation attacks against vulnerable individuals across jurisdictions – a worrying precursor to transnational enforced disappearances.

In addition to Altamides, Citizen Lab research has revealed a large-scale exploitation of these vulnerabilities by the commercial surveillance company Circles, which is an affiliate of NSO Group.[53] The company sells governments the ability to tap into SS7 networks to track targets

---

[48] Bill Marczak, John Scott-Railton, Siddharth Prakash Rao, Siena Anstis, and Ron Deibert(2020), "Running in Circles: Uncovering the Clients of Cyberespionage Firms Circles," *Citizen Lab* (December 1, 2020) <https://utoronto.scholaris.ca/server/api/core/bitstreams/82de8ca4-5759-4d54-8c9b-7270144c8950/content> .

[49] Stephanie Kirchgaessner (2020), "Revealed: Saudis suspected of phone spying campaign in US," *The Guardian* (March 29, 2020) <https://www.theguardian.com/world/2020/mar/29/revealed-saudis-suspected-of-phone-spying-campaign-in-us>

[50] Gabriel Geiger, Emmanuel Freudenthal, Crofton Black, et al. (2025), "Surveillance Secrets," *Lighthouse Reports* (October 14, 2025) <https://www.lighthousereports.com/investigation/surveillance-secrets/>.

[51] Gabriel Geiger, Emmanuel Freudenthal, Crofton Black, et al. (2025), "Surveillance Secrets," *Lighthouse Reports* (October 14, 2025) <https://www.lighthousereports.com/investigation/surveillance-secrets/>.

[52] Gabriel Geiger, Emmanuel Freudenthal, Crofton Black, et al. (2025), "Surveillance Secrets," *Lighthouse Reports* (October 14, 2025) <https://www.lighthousereports.com/investigation/surveillance-secrets/>.

[53] Bill Marczak, John Scott-Railton, Siddharth Prakash Rao, Siena Anstis, and Ron Deibert(2020), "Running in Circles: Uncovering the Clients of Cyberespionage Firms Circles," *Citizen Lab* (December 1, 2020) <https://utoronto.scholaris.ca/server/api/core/bitstreams/82de8ca4-5759-4d54-8c9b-7270144c8950/content>

in real time across jurisdictions, posing a significant threat to dissidents in exile or diaspora.[54] A number of state deployments of Circles' technology should concern this Committee and Working Group. Our research, and leaked exchanges between the parties, indicate a relationship between Circles and the United Arab Emirates (UAE) Supreme Council on National Security (SCNS)[55] – a serial abuser of surveillance technologies for the suppression of dissent and persecution of critical voices.[56] For example, the UAE's imprisonment of human rights activist Ahmed Mansoor was enabled by technology from Hacking Team,[57] Gamma Group's FinFisher, and NSO Group's Pegasus spyware.[58]

Beyond Saudi Arabia, Rwanda, and the UAE SCNS, the use of SS7 vulnerabilities has seemingly become a widespread means of state surveillance. Reporting suggests that Nigeria has used SS7 access to surveil opposition politicians and dissidents,[59] while Guatemala has used it to track journalists and activists.[60] Our research has identified the likely use of Circles by state actors in countries including Botswana, Chile, Mexico, Morocco, Thailand, and Zambia – all of whom have concerning records with regards to the use of digital surveillance for the purposes of suppressing dissent and/or effecting enforced disappearances across borders.[61]

---

[54] Bill Marczak, John Scott-Railton, Siddharth Prakash Rao, Siena Anstis, and Ron Deibert (2020), "Running in Circles: Uncovering the Clients of Cyberespionage Firms Circles," *Citizen Lab* (December 1, 2020) <https://utoronto.scholaris.ca/server/api/core/bitstreams/82de8ca4-5759-4d54-8c9b-7270144c8950/content>.

[55] Bill Marczak, John Scott-Railton, Siddharth Prakash Rao, Siena Anstis, and Ron Deibert (2020), "Running in Circles: Uncovering the Clients of Cyberespionage Firms Circles," *Citizen Lab* (December 1, 2020) <https://utoronto.scholaris.ca/server/api/core/bitstreams/82de8ca4-5759-4d54-8c9b-7270144c8950/content>

[56] Freedom on the Net 2025 (United Arab Emirates), *Freedom House* <https://freedomhouse.org/country/united-arab-emirates/freedom-net/2025>.

[57] Morgan Marquis-Boire (2012), "Backdoors are Forever: Hacking Team and the Targeting of Dissent?" *Citizen Lab* (October 10, 2012) <https://citizenlab.ca/2012/10/backdoors-are-forever-hacking-teaEverym-and-the-targeting-of-dissent/>.

[58] Bill Marczak and John Scott-Railton (2016), "The Million Dollar Dissident NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender," *Citizen Lab* (August 24, 2016) <https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/>.

[59] Ogala Emmanuel (2016), "INVESTIGATION: How Governors Dickson, Okowa spend billions on high tech spying on opponents, others," *Premium Times* (June 9, 2016) <https://www.premiumtimesng.com/investigationspecial-reports/204987-investigation-governors-dickson-okowa-spend-billions-high-tech-spying-opponents-others.html>.

[60] Angel Sas y Coralia Orantes (2018), "Illegal Government Spying: Here's Our Daily's Investigation (Part I)," *Nomada* (August 6, 2018) <https://nomada.gt/pais/la-corrupcion-no-es-normal/espionaje-ilegal-del-gobierno-aqui-esta-la-investigacion-de-nuestro-diario-parte-i/>.

[61] Bill Marczak, John Scott-Railton, Siddharth Prakash Rao, Siena Anstis, and Ron Deibert (2020), "Running in Circles: Uncovering the Clients of Cyberespionage Firms Circles," *Citizen Lab* (December 1, 2020) <https://utoronto.scholaris.ca/server/api/core/bitstreams/82de8ca4-5759-4d54-8c9b-7270144c8950/content>

Commercially Available Advertising Intelligence (AdInt)

The growing exploitation of SS7 vulnerabilities by malign operators has occurred alongside the expansion of 'Advertising Intelligence' (AdInt) as a means of surveilling dissidents across borders. AdInt is a term that describes the purchase and synthesis of commercially available advertising data for the purposes of geolocating and/or profiling particular individuals.[62]

This advertising data becomes available for surveillance due to privacy failures in the 'Real-Time Bidding' (RTB) process.[63] Every time an individual visits certain websites or uses certain applications, this data — which includes personal, behavioural, and geographic information collected over time from their internet and application usage — is transmitted to 'demand-side platforms' (DSPs). A DSP represents advertisers seeking to serve individually tailored/targeted ads based on that personal information. From there, based on the data they receive, the DSPs bid on behalf of advertisers for a slot on the website the individual is visiting. This constant real-time flow of personal data from users to advertising platforms is called the 'RTB Bidstream.'

A key problem underlying this system is that there are little-to-no real controls on who can sign up to receive this data (i.e., become a DSP) and what they can do with it when it is received.[64] This lack of control creates an opportunity for questionable operators to collect the information and sell it into a grey market for data frequented by malign actors, governments, or data brokers.[65] Research has indicated that purchasing commercially available advertising data for surveillance purposes has become a widespread practice of

[62] Johnny Ryan and Wolfie Chistl (2023) "Europe's hidden security crisis: How data about European defence personnel and political leaders flows to foreign states and non-state actors," *Irish Council for Civil Liberties* (November 14, 2023) <https://www.iccl.ie/wp-content/uploads/2023/11/Europes-hidden-security-crisis.pdf.>
[63] This paragraph's breakdown of 'Real Time Bidding' from the following report: Elizabeth Denham (in her capacity as UK Information Commissioner) (2019), "Update report into adtech and real time bidding," *UK Information Commissioner's Office* (June 20, 2019) at 10. <https://ico.org.uk/media2/migrated/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf>.
[64] Lena Cohen (2025), "Online Behavioral Ads Fuel the Surveillance Industry–Here's How," *Electronic Frontier Foundation* (January 6, 2025) <https://www.eff.org/deeplinks/2025/01/online-behavioral-ads-fuel-surveillance-industry-heres-how>.
[65] Lena Cohen (2025), "Online Behavioral Ads Fuel the Surveillance Industry–Here's How," *Electronic Frontier Foundation* (January 6, 2025) <https://www.eff.org/deeplinks/2025/01/online-behavioral-ads-fuel-surveillance-industry-heres-how>.

government intelligence and law enforcement agencies in the United States[66] and Europe.[67] Further, there is evidence to show that this data flows in large quantities to operators in Russia and China — whose national legal regimes allow the security agencies to access the data.[68]

The purchase of this commercially available data by state actors is particularly concerning for dissidents in exile and in the diaspora when paired with technologies and platforms that allow for its mass aggregation and analysis, producing specific insights into individual targets. Tactics can include the mapping of location data to determine a target's current location and historical movement patterns,[69] determinations about their in-person political activity,[70] or an analysis of online behavioural data for insights into their personal lives.[71]

The risk of location mapping using AdInt should be of particular concern to this Working Group. The release of the commercial surveillance software 'Patternz' showed how aggregated advertising data on approximately five billion people could be used to infer a particular targeted person's location, historical movements, and frequent contacts.[72] Recent work from *Le Monde* reaffirms how concerning this practice is, with their reporting showing how it can be used to track the movements and location of targeted government officials

---

[66] Sharon Bradford Franklin, Greg Nojeim and Dhanaraj Thakur (2021), "Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers," *Center for Democracy and Technology* (December 9, 2021) <https://cdt.org/insights/report-legal-loopholes-and-data-for-dollars-how-law-enforcement-and-intelligence-agencies-are-buying-your-data-from-brokers/>

[67] Thorsten Wetzling and Charlotte Dietrich, "Disproportionate use of commercially and publicly available data: Europe's next frontier for intelligence reform?," *Interface* (November 17, 2021) <https://www.interface-eu.org/publications/disproportionate-use-commercially-and-publicly-available-data-europes-next-frontier>.

[68] Johnny Ryan and Wolfie Chistl (2023) "Europe's hidden security crisis: How data about European defence personnel and political leaders flows to foreign states and non-state actors," *Irish Council for Civil Liberties* (November 14, 2023) <https://www.iccl.ie/wp-content/uploads/2023/11/Europes-hidden-security-crisis.pdf.>

[69] Joseph Cox (2024), "Inside a Global Phone Spy Tool Monitoring Billions," *404 Media* (January 24, 2024) <https://www.404media.co/inside-global-phone-spy-tool-patternz-nuviad-real-time-bidding/>; Martin Untersinger and Damien Leloup (2025), "How French Spies, police, and military personnel are betrayed by advertising data," *Le Monde* (December 13, 2025) <https://www.lemonde.fr/en/pixels/article/2025/12/13/how-french-spies-police-and-military-personnel-are-betrayed-by-advertising-data_6748453_13.html>.

[70] "FTC Complaint: In the Matter of MOBILEWALLA, INC.," *Federal Trade Commission* (January 6, 2025) at para 31 <https://www.ftc.gov/system/files/ftc_gov/pdf/2023196mobilewallacomplaint.pdf>.

[71] Michelle Boorstein and Heather Kelly (2023), "Catholic group spent millions on app data that tracked gay priests," *Washington Post* (March 9, 2023) <https://www.washingtonpost.com/dc-md-va/2023/03/09/catholics-gay-priests-grindr-data-bishops/>.

[72] Joseph Cox (2024), "Inside a Global Phone Spy Tool Monitoring Billions," *404 Media* (January 24, 2024) <https://www.404media.co/inside-global-phone-spy-tool-patternz-nuviad-real-time-bidding/>.

"down to a few metres."[73] Further, an FTC complaint against data brokerage Mobilewalla, which obtains data through the RTB Bidstream, showed how the company's use of precise location information allowed them to link specific individuals to political protests they attended.[74] Thus, the ability to precisely surveil individuals of interest has become commercially available to cybercriminals and states – providing a dangerous tool which may be used to effect enforced disappearances.

Ultimately, both telecommunications signalling exploitation and advertising-based geolocation enable states and state-related actors to locate individuals beyond their territorial borders at scale and with limited risk of detection. While the first method is particularly suited to real-time tracking, the latter enables long-term pattern analysis and target identification. Used together, these methods significantly reduce the practical barriers to identifying and physically apprehending individuals in exile. In the context of transnational repression, geolocation capabilities can facilitate surveillance, harassment, abduction, and enforced disappearance. Moreover, even when physical harm does not occur, the existence of these practices has significant chilling effects on human rights defenders and dissidents in exile and diaspora, restricts their freedom of movement, creates a state of fear and uncertainty, and increases self-censorship, which might push many to withdraw from public life or cease their human rights advocacy altogether.

What Legal Framework? The Unregulated Surveillance Market and the Responsibility of Host States

In this submission, we are particularly concerned with the human rights obligations of the states within which the transnational enforced disappearance takes place (i.e., the "host state"). Under international human rights law, host states are required to protect against and prevent human rights violations, including enforced disappearances.[75] In the context of a transnational enforced disappearance, this may include, for example, taking steps to prevent a real and immediate risk of an enforced disappearance, criminalizing enforced disappearances, conducting thorough and effective investigations into any enforced

[73] Martin Untersinger and Damien Leloup (2025), "How French Spies, police, and military personnel are betrayed by advertising data," *Le Monde* (December 13, 2025) <https://www.lemonde.fr/en/pixels/article/2025/12/13/how-french-spies-police-and-military-personnel-are-betrayed-by-advertising-data_6748453_13.html>.
[74] "FTC Complaint: In the Matter of MOBILEWALLA, INC.," *Federal Trade Commission* (January 6, 2025) at para 7, 31-32 <https://www.ftc.gov/system/files/ftc_gov/pdf/2023196mobilewallacomplaint.pdf>.
[75] Siena Anstis and Sophie Barnett (2022), "Digital Transnational Repression and Host States' Obligation to Protect Against Human Rights Abuses" (May 11, 2022) 14:2 *Journal of Human Rights Practice* <https://academic.oup.com/jhrp/article/14/2/698/6584375>

disappearance within the state's jurisdiction (and cooperating with other states in such investigations), and ensuring that the host state or its agents are not involved in facilitating an enforced disappearance.[76]

The obligation of host states to respect and ensure the human rights of individuals within their jurisdiction includes the obligation to take steps to prevent human rights violations that arise with digital transnational repression.[77] As the OHCHR noted in its 2018 report on the right to digital privacy, the responsibility of host states under international human rights law includes "a duty to protect persons within their jurisdictions from extraterritorial interference with their rights to privacy, such as means of interception of communications or hacking."[78] More specifically, this obligation would include taking measures to protect individuals against the type of targeted-surveillance activity that can arise in the context of an enforced disappearance.

As we illustrated above, the use of different surveillance technologies is likely to be a central part of any perpetrating state's planning and execution of a transnational enforced disappearance. The perpetrating state requires information regarding a victim's location prior to the anticipated enforced disappearance. Accurate information regarding the victim's location, their daily habits, and social networks greatly facilitates the state's ability to successfully execute an enforced disappearance, particularly in a transnational context where the state has to expend significant resources to undertake the enforced disappearances in and of itself (for example, by hiring local agents to undertake the enforced disappearance, sending in a state agent or convincing the host state to assist) at significant political risk.

In our prior submission to the Working Group, we underlined how states (and companies) must act to prevent the sale, transfer, and use of mercenary spyware technology absent sufficient regulation in place to control proliferation and ensure compliance with international human rights law. The situation has not changed significantly since 2022 and we have seen little progress towards effectively preventing the rights violations that arise with digital transnational repression. Research continues to show that the expanding private

---

[76] See, for example, the *International Convention for the Protection of All Persons from Enforced Disappearances* (2006), <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-protection-all-persons-enforced>.

[77] Siena Anstis and Sophie Barnett (2022), "Digital Transnational Repression and Host States' Obligation to Protect Against Human Rights Abuses" (May 11, 2022) 14:2 *Journal of Human Rights Practice* <https://academic.oup.com/jhrp/article/14/2/698/6584375>.

[78] OHCHR (2018), "The Right to Privacy in the Digital Age - Report of the United Nations High Commissioner for Human Rights" *OHCHR* (August 3, 2018) <https://www.ohchr.org/en/documents/thematic-reports/ahrc3929-right-privacy-digital-age-report-united-nations-high>.

market for surveillance technology, including mercenary spyware, remains largely unregulated.[79] Similarly, geolocation attacks exploiting telecommunications networks have long been identified as a weakness in our global telecommunications system. While efforts like those of United Kingdom (UK) regulators to ban the leasing of access to SS7 networks are a step in the right direction, more coordinated and comprehensive action is needed to sufficiently address this vulnerability.[80] Finally, the advertising industry has failed to protect the data of its customers — allowing for the emergence of a dangerous grey market for personal information. Meanwhile, documented violations of the industry's General Data Protection Regulation (GDPR) obligations have not been met with enforcement action[81] and legislative attempts to address the problem in the U.S. have languished for years in Congress.[82]

The continued failure to address the proliferation of these technologies and capabilities increases the likelihood that the technologies described in this report, as well as other surveillance technologies, will be repeatedly deployed in acts of transnational repression, including transnational enforced disappearances. In prior writing, we have proposed general recommendations regarding the measures that host states must take to address digital transnational repression and comply with their obligations under international human rights law.[83] These measures can be further refined in the context of enforced disappearances. We

[79] See, for example, Sarah Graham, Jen Roberts, and Nitansha Bansal (2025, "Mythical Beasts: Diving into the Depths of the Global Spyware Market" (September 10, 2025) *Atlantic Council* <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/mythical-beasts-diving-into-the-depths-of-the-global-spyware-market/>.

[80] Mark Sweney (2025), "Ofcom closes technical loophole used by criminals to intercept mobile calls and texts," *The Guardian* (April 22, 2025) <https://www.theguardian.com/technology/2025/apr/22/ofcom-bans-technical-loophole-used-by-criminals-to-intercept-mobile-calls-and-texts>.

[81] Elizabeth Denham (in her capacity as UK Information Commissioner) (2019), "Update report into adtech and real time bidding," *UK Information Commissioner's Office* (June 20, 2019) <https://ico.org.uk/media2/migrated/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf>.

[82] Emile Ayoub and Elizabeth Goitein (2024), "Closing the Data Broker Loophole" *Brennan Center for Justice* (February 13, 2024) <https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole>.

[83] Siena Anstis and Sophie Barnett (2022), "Digital Transnational Repression and Host States' Obligation to Protect Against Human Rights Abuses" (May 11, 2022) 14:2 *Journal of Human Rights Practice* <https://academic.oup.com/jhrp/article/14/2/698/6584375>; Noura Al-Jizawi, Siena Anstis, Sophie Barnett, Sharly Chan, Niamh Leonard, Adam Senft, and Ron Deibert (2022), "Psychological and Emotional War: Digital Transnational Repression in Canada," *The Citizen Lab* (March 1, 2022) <https://citizenlab.ca/wp-content/uploads/2022/03/Report151-dtr_022822.pdf>; Noura Aljizawi, Siena Anstis, Marcus Michaelsen, Veronica Arroyo, Shaila Baran, Maria Bikbulatova, Gözde Böcü, Camila Franco, Arzu Geybulla, Muetter Iliqud, Nicola Lawford, Émilie LaFlèche, Gabby Lim, Levi Meletti, Maryam Mirza, Zoe Panday, Claire Posno, Zoë Reichert, Berhan Taye, and Angela Yang (2024), "No Escape: The Weaponization of Gender for the Purposes of Digital Transnational Repression," *The Citizen Lab* (December 2, 2024) <https://citizenlab.ca/wp-content/uploads/2024/12/Report180-noescape112924.pdf>.

offer suggestions both for the Committee and the Working Group, as well as for host states and businesses:

Recommendations to the Working Group and Committee

- **In its work on enforced disappearances, the Committee should include analysis of how digital technologies are used in enforced disappearances and issue recommendations which reflect this analysis.** This could include identifying cross-border acts of enforced disappearances as an act of transnational repression when reviewing individual complaints, and highlighting any facts related to the use of digital technologies in enforced disappearances. It could also include specific analysis on the role of digital technologies in enforced disappearances when assessing state reports and the measures states must take to address enforced disappearances. For example, the Committee (and Working Group) could issue specific recommendations to host states in the context of transnational enforced disappearances that include taking measures to strengthen the digital security of vulnerable groups and the adoption of legislative measures that expressly penalizes the transnational use of digital technologies as part of any surveillance activity by a foreign state.

- **The Working Group should include the issue of digital technologies as a dimension in its work around enforced disappearances.** This inclusion could contribute to highlighting the use of digital technologies in the context of an enforced disappearance in communications with governments; requesting governments to examine all aspects of an enforced disappearance, including, more specifically, the use of digital technologies in facilitating enforced disappearances; and including a section in country reports that reviews how digital technologies are being used in such human rights violations and/or what protective measures states need to adopt to ensure that transnational use of digital technologies to facilitate enforced disappearances is addressed by host states. In the subsequent bullets, we highlight some of the measures that the Working Group could underline for states to act upon.

Recommendations to host states

- **Host states need to adequately investigate enforced disappearances within their jurisdiction and seek to understand and document how digital technologies are implicated.** Perpetrating states will use targeted surveillance as a mechanism to prepare an enforced disappearance. We anticipate that the use of targeted surveillance to achieve acts of transnational repression such as enforced disappearances or killings

will only increase as these tools become increasingly widely available. Host states need to be cognizant that the deployment of surveillance technology is a part of the playbook of perpetrating states engaging in transnational repression and react accordingly. Under international human rights law, host states are under an obligation to adequately investigate enforced disappearances that arise on their territory. This obligation should be interpreted to include adequate investigation into the role of surveillance technology in facilitating the offence. The host state should seek to understand how surveillance technology played a role in the facilitation of the offence and what measures need to be taken by the state to prevent such abuse.

- **Host states should ensure that victims are able to seek a remedy against the perpetrating state and companies that facilitate transnational surveillance.** Host states should ensure that state immunity laws do not prevent the victim (or their relatives) of a transnational enforced disappearance from seeking a remedy against the state that perpetrated the act. Further, host states should ensure that victims can also seek a remedy against surveillance companies that are implicated in a transnational enforced disappearance by removing jurisdictional hurdles. Such litigation may be helpful in shedding light on how surveillance technology is used in the process of an enforced disappearance by providing a forum for discovery and fact finding.

- **Host states need to provide assistance to individuals and communities impacted by enforced disappearances and ensure that they can adequately protect themselves against targeted surveillance.** By ensuring that the digital dimension of an enforced disappearance is examined and accounted for during investigations into enforced disappearances, host states will be better equipped to prevent the weaponization of surveillance technology against individuals and community members that are at risk of enforced disappearances. Host states should ensure that individuals and communities have access to tailored digital security advice and training that can contribute to helping prevent perpetrating states from successfully hacking and tracking potential victims and their families or broader community. Host states should ensure there is a point of contact to provide individualized assistance to high-risk individuals such as those likely to be targeted in transnational enforced disappearances or killings. Our general recommendations regarding how states should respond to digital transnational repression equally apply in the context of addressing the digital dimensions of transnational enforced disappearances.[84]

[84] Siena Anstis and Sophie Barnett (2022), "Digital Transnational Repression and Host States' Obligation to Protect Against Human Rights Abuses" (May 11, 2022) 14:2 *Journal of Human Rights Practice* <https://academic.oup.com/jhrp/article/14/2/698/6584375>; Noura Al-Jizawi, Siena Anstis, Sophie Barnett, Sharly Chan, Niamh Leonard, Adam Senft, and Ron Deibert (2022), "Psychological and Emotional War: Digital

- **Host states need to address the role of companies that facilitate enforced disappearances through the use of targeted surveillance technology.** Host states must take steps to ensure that companies in their jurisdiction are not contributing to or facilitating the use of surveillance technology in enforced disappearances by, among other measures, tightly regulating the production, sale and transfer of surveillance technology. This includes implementing strict export controls and banning the sale of spyware or other surveillance technology to states that are likely to use them in violation of human rights, such as in the context of transnational enforced disappearances. Host states must also take measures to hold companies and executives to account through, for example, targeted sanctions or criminal proceedings. We have made specific recommendations regarding the regulation of the spyware market in prior articles and reports.[85]

- **Host states should address the surveillance vulnerabilities inherent in AdInt through comprehensive data rights and privacy legislation, paired with effective enforcement.** The challenge of AdInt-enabled surveillance is rooted in the fact that large technology companies and advertisers are not processing data in a responsible manner, allowing it to flow indiscriminately to a range of actors who may either use it for surveillance purposes or resell it on a grey market.[86] Legislation that creates strict limitations on who can process data, as well as why and how they can do it, would stop this haphazard outward flow of personal data from the RTB Bidsteam – thereby cutting the AdInt market off at its source. Such regulation has to be accompanied with effective enforcement. Jurisdictions with existing legislation, such as the U.K. and the European Union (E.U.), should respectively act on calls by the U.K. Information

---

Transnational Repression in Canada," *The Citizen Lab* (March 1, 2022) <https://citizenlab.ca/wp-content/uploads/2022/03/Report151-dtr_022822.pdf>; Noura Aljizawi, Siena Anstis, Marcus Michaelsen, Veronica Arroyo, Shaila Baran, Maria Bikbulatova, Gözde Böcü, Camila Franco, Arzu Geybulla, Muetter Iliqud, Nicola Lawford, Émilie LaFlèche, Gabby Lim, Levi Meletti, Maryam Mirza, Zoe Panday, Claire Posno, Zoë Reichert, Berhan Taye, and Angela Yang (2024), "No Escape: The Weaponization of Gender for the Purposes of Digital Transnational Repression," *The Citizen Lab* (December 2, 2024) <https://citizenlab.ca/wp-content/uploads/2024/12/Report180-noescape112924.pdf>.

[85] Ron Deibert (2022), "The Autocrat in Your iPhone: How Mercenary Spyware Threatens Democracy" *Foreign Affairs* (December 12, 2022) <https://www.foreignaffairs.com/world/autocrat-in-your-iphone-mercenary-spyware-ronald-deibert>; Sarah McKune and Ron Deibert (2017) , "Who's Watching Little Brother?: A Checklist for Accountability in the Industry Behind Government Hacking" *Citizen Lab* (March 2, 2017) <https://citizenlab.ca/wp-content/uploads/2017/03/citizenlab_whos-watching-little-brother.pdf>.

[86] Johnny Ryan and Wolfie Chistl (2023) "Europe's hidden security crisis: How data about European defence personnel and political leaders flows to foreign states and non-state actors," *Irish Council for Civil Liberties* (November 14, 2023) <https://www.iccl.ie/wp-content/uploads/2023/11/Europes-hidden-security-crisis.pdf.>

Commissioner's Office[87] and E.U. litigants[88] to close enforcement gaps that currently allow AdInt market actors to evade effective regulation.

- **Host states should regulate telecommunications, ensure strong enforcement of regulations, and actively prevent trafficking of private information.** As a starting point, host states should set clear regulations for telecommunications operators governing their compliance with cybersecurity architecture, disclosure of security concerns, and foreign-operator access to subscriber-identifying information.[89] Further, law enforcement should actively engage in operations to prevent the trafficking of private subscriber identifiers on places like the dark web.[90]

Recommendations to businesses

- **Companies whose services and products are exploited by spyware companies should continue to take an aggressive response to counter these practices.** Technology companies providing legitimate services and products – e.g., Apple, Google, and Meta – should continue to take action to deter the activities of spyware companies and to ensure greater protection for high-risk groups. This includes pursuing litigation against spyware companies to stop the abuse of these companies' services and products; providing information to civil society groups regarding these threats for further investigation; and issuing notifications or warnings to potentially affected users regarding state-linked threats. These suggestions should be read in conjunction with our prior recommendations, which include recommendations aimed at companies that produce surveillance technologies.[91]

---

[87] Elizabeth Denham (in her capacity as UK Information Commissioner) (2019), "Update report into adtech and real time bidding," *UK Information Commissioner's Office* (June 20, 2019) at 15 <https://ico.org.uk/media2/migrated/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf>.
[88] "ICCL's lawsuit takes aim at Google, Facebook, Amazon, Twitter, Verizon, AT&T and the entire online advertising/tracking industry by challenging industry rules." *Irish Council of Civil Liberties* (June 15, 2021) <https://www.iccl.ie/rtb-june-2021/>.
[89] Gary Miller and Christopher Parsons (2023), "Finding You: The Network Effect of Telecommunications Vulnerabilities for Location Disclosure," *Citizen Lab* (October 26, 2023) <https://citizenlab.ca/2023/10/finding-you-teleco-vulnerabilities-for-location-disclosure/#conclusion>.
[90] Gary Miller and Christopher Parsons (2023), "Finding You: The Network Effect of Telecommunications Vulnerabilities for Location Disclosure," *Citizen Lab* (October 26, 2023) <https://citizenlab.ca/2023/10/finding-you-teleco-vulnerabilities-for-location-disclosure/#conclusion>.
[91] Siena Anstis, Dr. Ronald J. Deibert, Émilie LaFlèche, and Jon Penney (2022), "Submission of the Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto) to the United Nations Working Group on Enforced or Involuntary Disappearances," *The Citizen Lab* (June 18, 2022) <https://citizenlab.ca/wp-content/uploads/2022/07/Submission-of-the-Citizen-Lab-Munk-School-of-Global-Affai

- **Standards setting bodies for the digital advertising sector should amend protocols to ban the transmission of sensitive behavioural or location data.** Standard setting bodies like IAB TechLab and Google, which set the rules for the entirety of real-time bidding data broadcasts, should ban the sharing of sensitive behavioural or precise location data with demand-side platforms.[92] This action would also have the effect of cutting off the grey market for commercially available advertising data off at its source, limiting its access by malign state actors or cybercriminals.

- **Mobile operators should enhance security measures related to SS7 exploitations.** Mobile operators should adopt, implement, and demonstrably comply with recognized cybersecurity guidelines and frameworks, such as zero-trust architectures; report cybersecurity incidents and attacks in a timely manner; accept accountability where their networks are exploited by surveillance actors; work towards the development of security agreements and accreditation schemes; and conduct regular penetration testing to identify and remediate vulnerabilities.[93]

Conclusion

Enforced disappearances – both domestic and transnational – have been facilitated by the use of targeted surveillance technology deployed by perpetrating states. As the examples highlighted in this submission illustrate, access to targeted surveillance technologies like spyware make it increasingly possible for perpetrating states to reach across borders and plan the enforced disappearance of a victim. Such surveillance tools enable perpetrating states to figure out where a victim is located, what their daily routines and habits are, and map out their personal and professional networks. With this valuable information in hand, a perpetrating state is in the position to – successfully – undertake a transnational enforced disappearance. We emphasize in this submission that host states, in particular, need to anticipate the use of targeted surveillance in acts of enforced disappearance and take measures to address it. This includes undertaking thorough investigations into enforced disappearances and accounting for the digital dimension of these offences; providing specific

rs-University-of-Toronto-to-the-United-Nations-Working-Group-on-Enforced-or-Involuntary-Disappearances.pdf >.

[92] Johnny Ryan and Wolfie Chistl (2023) "Europe's hidden security crisis: How data about European defence personnel and political leaders flows to foreign states and non-state actors," *Irish Council for Civil Liberties* (November 14, 2023) <https://www.iccl.ie/wp-content/uploads/2023/11/Europes-hidden-security-crisis.pdf.>

[93] Gary Miller and Christopher Parsons (2023), "Finding You: The Network Effect of Telecommunications Vulnerabilities for Location Disclosure," *Citizen Lab* (October 26, 2023) <https://citizenlab.ca/2023/10/finding-you-teleco-vulnerabilities-for-location-disclosure/#conclusion>.

and tailored digital security support and training to impacted or likely impacted communities; and ensuring that surveillance companies cannot export these technologies to regimes that are likely to use them in violation of international human rights law.