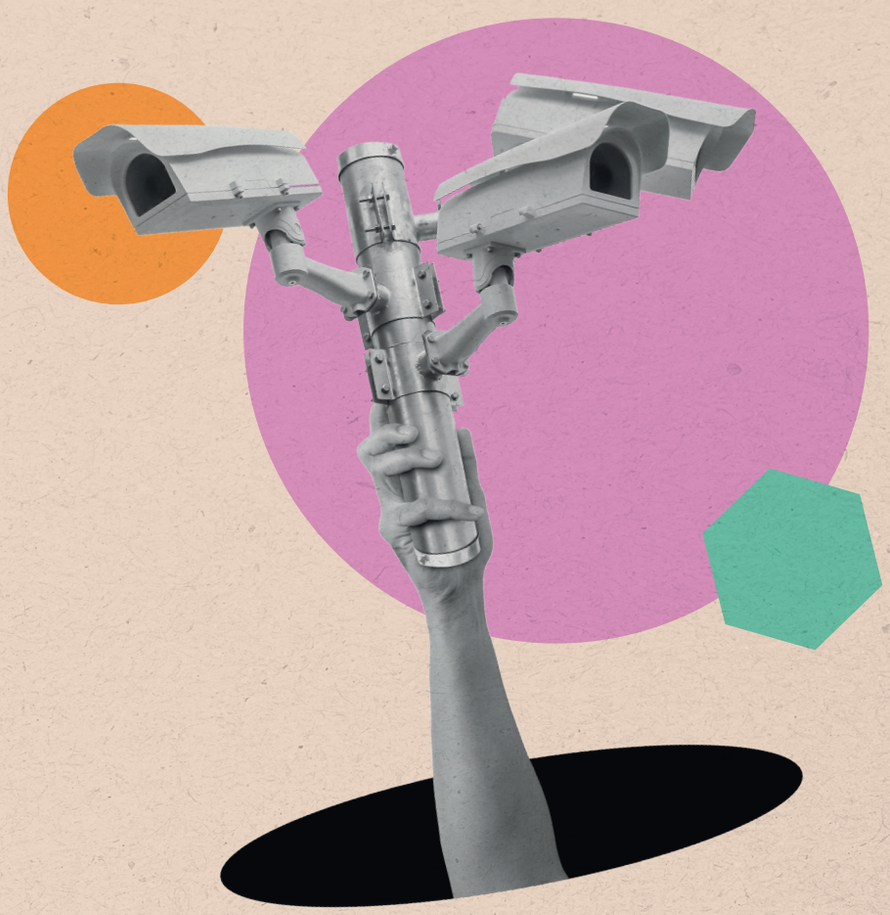
United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism

Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach

April 2023



UNITED NATIONS
HUMAN RIGHTS
SPECIAL PROCEDURES
SPECIAL RAPPORTEURS, INDEPENDENT EXPERTS & WORKING GROUPS

Acknowledgements

This position paper on **Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach** is presented by **Professor Fionnuala Ní Aoláin, the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism.**

Work on this report was led by Adriana Edmeades Jones, Legal Advisor to the Special Rapporteur. Facilitation and publication management for this work was provided by the Human Rights Center at the University of Minnesota Law School, which provides ongoing programme management support to the mandate of the Special Rapporteur.

Facilitation and programme management for the work of the Special Rapporteur are led by Michelle Erazo and Karen Reyes Tolosa, Human Rights Officer and Associate Human Rights Officer, Office of the High Commissioner for Human Rights (OHCHR).

This paper builds on the ground-breaking revelations of the investigative journalism initiative 'The Pegasus Project' led by Amnesty International and Forbidden Stories, who worked together with a number of media outlets, including the Organized Crime and Corruption Reporting Project. It also owes much to the longstanding and outstanding work of The Citizen Lab at the University of Toronto, and the tireless efforts of many other human rights defenders and members of civil society who have worked to expose the use of spyware and the human rights harms that it has caused. Finally, we acknowledge and endorse the prior work of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Professor David Kaye.

Contents

Section		Page
01	Executive Summary	06
02	Introduction	10
03	Part I: Understanding Surveillance Technology Designed and Deployed for Counter-Terrorism	17
	- Violations of the Right To Life/Exposure to Physical Violence (Including Sexual Violence), Unlawful Arrest and/or Harrassment from Government or Private Actors	24
	- Disprorportionate Interference with Individuals' Right to Privacy	34
	- Disprorportionate Interference with the Right to Freedom of Expression, Freedom of Association, and Freedom of Religion	40
	- The Production and Entrenchment of Particular Gender Harms, Including Direct Harms to Women and Girls and LGBTI+ Persons	44
	- Interference with the Integrity of Documentary Records and Evidence, Undermining Procedural Fairness and Rule of Law	49
	- Obstacles to Obtaining Effective Remedies	53
04	Part II: Current Regulatory Frameworks Relevant to the Trade in Surveillance Technology	56
	- Regulation of Businesses Engaged in Surveillance Technology Industry	57
	- Regulation of States Allowing Trade in Surveillance Technology	74
05	Part III: The Way Forward to More Effective International Regulation of Surveillance Technology	83

01 Executive Summary

Sophisticated surveillance technology developed for counter-terrorism and national security purposes has increasingly become a focus of international concern thanks to a spate of revelations demonstrating that such tools are in fact being used to spy upon politicians, journalists, human rights activists, lawyers, and ordinary citizens with no links to terrorism and who pose no national security threat. Recent leaks - most notably in respect of the widespread use of the Pegasus spyware technology - show that, whatever the justification for the intended application of this technology, something is fundamentally wrong in practice. Intrusive covert technology for surveillance of the content of individuals' digital communications, and other information including metadata (location, duration, source, and contacts) - commonly known as 'spyware' - has proliferated internationally out of all control and poses substantial risks to the promotion and protection of human rights.

This paper examines why we are in this position, demonstrating that this uniquely invasive and powerful technology and the flourishing international trade in spyware all pose significant challenges for the conventional mechanisms which are meant to monitor the trade in potentially harmful products and mitigate adverse human rights risks. The way in which the trade and use of these tools cross borders, and the relationships between State agencies and private contractors, create substantial obstacles for conventional regimes for legal accountability, while the clandestine use of the technology and its capacity to modify or erase its tracks threatens ordinary approaches to evidence and investigation. This paper seeks to raise awareness of the significant human rights challenge posed by the use of spyware, and the weaknesses it has exposed in the international legal and regulatory system we rely upon for the protection of human rights and fundamental freedoms.

The current response to the challenge posed to human rights by the extremely powerful tools of the contemporary spyware industry is fractured and inadequate. Direct approaches to the voluntary responsibility of corporations developing and selling the technology rely upon the UN Guiding Principles on Business and Human Rights, the effectiveness of which is undermined by the absence of a binding enforcement arm. Domestic private law doctrines form an inconsistent patchwork, with ample room for argument about degrees

of responsibility along transnational production chains, how human rights harms equate to (or diverge from) traditional models of physical harm, and how relationships between private entities and foreign sovereign entities ought to be dealt with. They also necessitate victims of unlawful surveillance having the knowledge and the means to use litigation to hold private companies to account. At the same time the export control system was developed for the radically different context of conventional arms. It grants exporting States generous latitude in their decision-making, providing the conditions for confusion, inconsistency, and arbitrage between jurisdictions.

Where to from here? A range of ongoing efforts to tighten and clarify standards and protections are to be welcomed. Some voices call for a blanket ban on the trade in and use of spyware. While recognizing the particular threat posed by spyware, and not ruling out the conclusion that a ban may well be required, this paper urges the international community to take a bold and transformative approach to the regulation of this technology. This paper makes a set of concrete and innovative recommendations for a human-rights compliant regulatory response to the challenges raised by the international proliferation of spyware technology, which includes ways to incentivize and responsibilize manufacturers and short-circuit the evidential problems encountered in regulating spyware. Further, this paper proposes a mechanism of mutual international obligation and recognition as a way to minimize international regulatory arbitrage.

A human rights analysis of the use of spyware in the counter-terrorism context suggests that spyware technology must at a minimum: (a) allow for users to specifically target certain data and metadata, rather than automatically monitor and record all data and metadata; (b) avoid automatically accessing data relating to contacts of targeted individuals, unless users specifically require that additional information for investigative purposes; (c) engineer mechanisms to prevent harmful use, such as flagging systems and 'kill switches' in cases of apparent misuse; and, in any event, (d) create an indelible, permanent, and uneditable auditable record of what actions have been taken by the user of the spyware, including any interferences/modifications of data/metadata, when those occurred, and by whom they were effected so that the use of the tool can be verified, and its human rights compliance assessed after the fact by judicial authorities. Part of that indelible

and uneditable record must be some form of identifier or watermark such that judicial authorities overseeing complaints may verify the producer of spyware alleged to have been used against a victim and the customer to which that spyware was originally supplied and, from such source, can compel disclosure of the auditable record such that the legality of any use complained of can be adequately reviewed. Spyware which fails to display such features cannot, however otherwise tightly regulated, be capable of human rights compliance.

Spyware technology is currently being produced and deployed without a rigorous regulatory framework capable of responding to its unique characteristics and substantial threat to human rights. The international community must heed the call to act now.

“I’ve spent my entire career working to defend people’s rights, and now a government is trying to use me as a tool to undermine them. It’s paralyzing and chilling, and it’s why the stakes are so high when it comes to ending unlawful surveillance.”

- Lama Fakih
Director of the Middle East and North Africa Division,
Human Rights Watch

Source: HRW, “I was Attacked with Pegasus”, 28 January 2022, https://www.hrw.org/news/2022/01/28/i-was-attacked-pegasus.

02 Introduction

1. This paper examines the contemporary challenge to human rights posed by the worldwide proliferation and misuse of sophisticated intrusive cyber surveillance technologies originally justified by or intended for counter-terrorism and national security purposes. These powerful and innovative technologies are capable of providing law enforcement, militaries and security services with incisive investigative and monitoring tools to disrupt terrorist violence and bring perpetrators to justice. The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (Special Rapporteur) is profoundly concerned that these technologies are routinely being deployed and misused by States, private actors, and criminal groups, posing serious harm to the safety, security, and fundamental freedoms of among others, ordinary citizens, political leaders and activists, human rights defenders, lawyers, business leaders, minorities, humanitarians, and journalists worldwide. Responsibility for this grave problem lies with corporations and private entities that knowingly provide such technologies directly to rights-violating regimes or fail to exercise due diligence as to the end use of their products; with State agencies which misuse these technologies in violation of international and domestic law; and with States which either actively facilitate, or fail to prevent, the trade of such technologies into the wrong hands.

2. The proliferation and misuse of surveillance technology is of particular concern to the Special Rapporteur because it vividly demonstrates the risks to human rights which persist in the counter-terrorism and security space due to broad and ill-defined counter-terrorism objectives, providing cover for the systematic disregard of human rights by States and private actors. Counter-terrorism activities appear to enjoy a political safe-space as exceptional activities to which ordinary rules and the fundamental rule of law need not necessarily apply, while domestic legislation almost universally excludes the counter-terrorism context from full scrutiny or allows counter-

terrorism and security justifications to clothe activities with legitimacy despite their lack of respect for human rights. The Special Rapporteur has consistently commented upon the lack of an internationally agreed definition of terrorism, which has left a legal and normative 'black hole' within which States have extraordinary leeway to define for themselves counter-terrorism objectives and emergencies and exceptional powers to justify their own actions.[1] States continue to exploit these loose counter-terrorism boundaries for other purposes, including the silencing of dissent, the persecution of opposition, and the suppression of evidence of wrongdoing.[2] While the Special Rapporteur has advocated a precise and tightly defined model definition of terrorism[3], few States have adopted this circumscribed definition. The result is that the counter-terrorism space, for which sophisticated surveillance technology is developed and marketed, and within which State agencies deploy that technology, is fertile ground for the systematic violation of human rights.

---

[1] See, e.g.: A/HRC/31/65, [21], [24], and [27]; A/HRC/37/52, [33], [36], and [66]; and A/HRC/40/52, [34]-[35]. The vagueness of legislation addressing terrorism, and the problematic latitude it affords States, has also been a consistent subject of criticism by regional human rights courts: see, for instance: *Big Brother Watch v United Kingdom* [2021] ECHR 439 and *OOO Flavus and ors v Russian Federation* [2020] ECHR 463.

[2] A/HRC/40/52.

[3] A/HRC/16/51, [28].

3. In recent years, the widespread misuse of surveillance technology purportedly in service of counter-terrorism and national security objectives, with concerning disregard for fundamental human rights protections, has been exposed in dramatic fashion. Most recently, the scandal relating to the use by repressive regimes of Pegasus[4] – a surveillance software program manufactured by the cyber-intelligence company NSO Group – has prompted the European Parliament to launch a committee of inquiry into the trade in such technology,[5] and has led to litigation brought against the NSO Group and its State clients by corporations[6] and individuals claiming to be victims of unlawful targeting.[7]

4. In light of these revelations, a growing number of voices in the international human rights community have supported the call for a more robust, human rights-compliant regulatory framework for the use, sale, and transfer of surveillance technology—and in the meantime, a moratorium on the trade and transfer of such technology. The UN High Commissioner for Human Rights has called for a better, human rights-based system to regulate the spyware trade, including mechanisms for fixing responsibility for human rights breaches on private spyware producers by '*requir[ing] by law that the companies involved meet their human rights responsibilities, are much more transparent in relation to the design and use of their products, and put in place more effective accountability measures.*'[8] In the meantime, the High Commissioner has also called for a suspension of the trade in surveillance technology to '*allow States to work on an export and control regime, as well as to boost legal frameworks securing privacy.*'[9] Similarly, the UN Special Rapporteur on the promotion and protection of the right to freedom of expression, the UN Special Rapporteur on the situation of human rights defenders, the UN Special Rapporteur on the rights to

---

[4] See: 'Takeaways from the Pegasus Project,' *The Washington Post* (18 July 2021), available at: https://www.washingtonpost.com/investigations/2021/07/18/takeaways-nso-pegasus-project/; and S Kirchgaessner et al., 'Revealed: Leak Uncovers Global Abuse of Cyber-Surveillance Weapon,' *The Guardian* (18 July 2021), available at: https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus

[5] See: European Parliament decision of 10 March 2022 on setting up a committee of inquiry to investigate the use of the Pegasus and equivalent surveillance spyware, and defining the subject of the inquiry, as well as the responsibilities, numerical strength and term of office of the committee (2022/2586(RSO)). As of October 2022, the committee has conducted hearings on topics including the use of spyware in Poland and Greece, the sale of spyware by Israel-based companies (including NSO) to EU governments. See: https://www.europarl.europa.eu/committees/en/pega/home/highlights

[6] See, e.g., the litigation brought by WhatsApp in the US federal courts for the Northern District of California: Case No. 19-cv-07123-PJH *WhatsApp Inc., et al v NSO Group Technologies Ltd, et al.*

[7] See, e.g., the litigation brought by Mr Ghanem al-Masarir against the Kingdom of Saudi Arabia ('KSA') in the English High Court. In an August 2022 judgment on the preliminary issue of whether the KSA was immune from suit under the international law doctrine of state immunity (incorporated in English law by the State Immunity Act 1978), the High Court held that the KSA was not immune and that the claim could advance to the substantive stage: *Al-Masarir v Kingdom of Saudi Arabia* [2022] EWHC 2199 (QB).

[8] OHCHR, 'Use of spyware to surveil journalists and human rights defenders,' 19 July 2021, available at: https://www.ohchr.org/en/2021/07/use-spyware-surveil-journalists-and-human-rights-defendersstatement-un-high-commissioner

freedom of peaceful assembly and of association, and members of the UN Working Group on Business and Human Rights jointly observed that '*[i]n recent years we have repeatedly raised the alarm about the danger that surveillance technology poses to human rights. Once again, we urge the international community to develop a robust regulatory framework to prevent, mitigate and redress the negative human rights impact of surveillance technology and pending that, to adopt a moratorium on its sale and transfer.*'[10] Support for an interim moratorium was recently repeated by the Office of the High Commissioner for Human Rights in the 2022 'Right to Privacy in the Digital Age' report.[11] In April 2022, the Republic of Costa Rica in April 2022 became the first State to join the call for a moratorium on the trade in spyware technology,[12] while a broad coalition of civil society reiterated the demand for a moratorium at the World Economic Forum meeting in Davos in May 2022.[13]

5. Some experts have gone further, including Professor David Kaye, formerly Special Rapporteur on the promotion and protection of the right to freedom of expression. Professor Kaye has observed that the problem is not so much that the '*system of control and use of targeted surveillance technologies is broken' but that '[i]t hardly exists,*'[14] since even though theoretically human rights should limit misuse, there is no effective framework to enforce those limitations.[15] He has suggested key features of existing domestic and international law which, if enjoying greater compliance, would deliver real benefits in terms of mitigating misuse of surveillance technology. But he has also recognized that the inherent risks posed by spyware may be such that a total ban is required, albeit that, as with the precedent of the comprehensive international prohibition on land mines, such a ban may take time to attract support.[16]

---

[9] Committee on Legal Affairs and Human Rights, Parliamentary Assembly of the Council of Europe, Statement by UN High Commissioner for Human Rights (14 September 2021), available at: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27455&LangID=E

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

[11] A/HRC/51/17, [19].

[12] 'Stop Pegasus: Costa Rica is the first country to call for a moratorium on spyware technology,' Access Now (13 April 2022), available at: https://www.accessnow.org/costa-rica-first-country-moratorium-spyware/

[13] 'Human rights leaders at Davos 2022: spyware is a weapon,' Press Conference, available at: https://www.accessnow.org/spyware-davos-press-conference/

[14] A/HRC/41/35, [46].

[15] A/HRC/41/35, [46].

[16] Prof D Kaye, 'Here's what world leaders must do about spyware,' 13 October 2022, Committee to Protect Journalists, available at: https://cpj.org/2022/10/david-kaye-what-world-leaders-must-do-about-spyware/

6. This position paper by the Special Rapporteur sets out the views of her mandate on the regulation of the sale, use and transfer of spyware technology and calls for the establishment of human rights-respecting regulatory mechanisms. She provides specific recommendations on how this might be achieved. **Specifically, the paper proposes draft text for an international commitment or treaty to give effect to such regulation.**

7. The Special Rapporteur does not rule out that States may come to take the view that a total ban on spyware is justified but heeds the High Commissioner's call to investigate and work towards a human rights-compliant regulatory system for the sale, use and transfer of spyware technology either as a precursor to such a ban or as a means to ensure protection for human rights without the necessity for one. Working towards such a regulatory system may occur alongside a moratorium on spyware, and does not undermine the growing demand at the international level for at least a temporary cessation of the trade in, and use of, such technology pending a new and robust regulatory approach. Accordingly, this paper responds directly to the High Commissioner's request for the development of human rights-respecting regulatory mechanisms, and seeks to provide a basis for concretizing if, and how, human rights and fundamental freedoms may be protected in a world with spyware technology.

8. **The purpose of this paper is to propose a structure to regulate and incentivize human rights compliance in the use and trade in spyware.** The paper does this by considering in detail the risks which particular aspects of the trade raise, and surveying the adequacy and effectiveness of existing and potential mechanisms for oversight and redress of human rights violations. The paper considers a range of case studies revealing how the use of spyware, and its trade, has been dealt with in the regulatory, legislative, and judicial spheres. Informed by this work, this paper makes concrete recommendations as to the necessary features of a future regulatory regime. The intention is that States and international organizations may use the recommendations in this paper as a framework for the design of the next generation of international regulation of this vital but challenging field.

9. This paper is produced pursuant to the mandate of the Special Rapporteur under Human Rights Council Resolution 15/15 to '*make concrete recommendations on the promotion and protection of human rights and fundamental freedoms while countering terrorism.*'[17]

10. This paper proceeds in three parts. First, it provides a broad overview of the specific risks for human rights posed by the international trade in spyware technology purportedly designed and deployed for counter-terrorism purposes. Second, it considers the state of current regimes to govern and respond to the trade in such technology, and assesses their effectiveness in addressing human rights risks. And third, it makes recommendations for the sort of new regulatory regime required if States are to prevent the violations of human rights which have become synonymous with the practices of the spyware industry. The recommendations set out what the contours for the next stage of international regulation should be, including by way of a draft set of commitments which States are encouraged to adopt.

11. This paper will contribute to the understanding of the risks raised by the current and emerging generation of counter-terrorism surveillance technologies. It will also provide international entities and civil society stakeholders with a coherent set of recommendations for an international response leading to the adoption of a binding multilateral treaty governing the development, trade, and deployment of counter-terrorism spyware technology in a human rights-respecting manner.

[17] A/HRC/RES/15/15, [2(a)].

“This is more than just eavesdropping, it’s terrifying. The spyware takes complete control over the phone. It can make calls to anybody, send messages and it can download content... Whoever is operating the surveillance equipment could phone somebody in the Islamic State [ISIL/ISIS] and then say I have been dealing with terrorists.”

Executive director of the Bisan Centre for Research and Development, Palestine

Source: “Palestinian rights activists defiant over Israeli spyware hacks”, *Al Jazeera* (14 November 2021), https://www.aljazeera.com/news/2021/11/14/palestinian-rights-activists-defiant-over-israeli-spyware-hacks

03 Part I: Understanding Surveillance Technology Designed and Deployed for Counter-Terrorism

12. The twin twenty-first century forces of the rapid increase in the capacity and complexity of computer hardware and software combined with the substantial expansion in funding for, and prominence of, State counter-terrorism programmes has led to the development of a wide range of sophisticated surveillance technologies either directed to, or suitable for, counter-terrorism purposes. Standard practice in respect of counter-terrorism and criminal investigation promoted by multilateral organizations such as the Council of Europe and the International Criminal Police Organization ('Interpol') calls for routine surveillance and collection of data via a range of hardware and software tools for investigative analysis.[18] The capacity for such mass surveillance as the default tool for investigation has been dramatically increased by a series of converging trends in recent years: the precipitous decline in the cost of technology and data storage; the ubiquity of digital devices and connectivity; and the exponential increase in computers' processing power.

13. The explosion of the surveillance technology industry in the twenty-first century has been partly due to the significant flows of funding into the counter-terrorism field. It has also followed from the extraordinary powers that State agencies have arrogated to themselves on the purported basis that the imperatives of counter-terrorism justify ubiquitous surveillance and government intrusion as a preventative and investigative tool.[19] That intrusion is typically presented as targeted only against certain risk groups, typically vaguely and problematically defined by reference to (often discriminatory)[20]

---

[18] See, e.g.: Cybercrime Programme Office of the Council of Europe (C-PROC), 'Standard Operating Procedures for the Collection, Analysis, and Presentation of Electronic Evidence' (September 2019).

[19] As noted by the former Special Rapporteur, Mr Emmerson: A/69/397, [19].

[20] A/HRC/43/46, [28]-[34].

assumptions as to perceived risk of future harm. Such risk assessments are often poorly empirically based and their methodologies weak and ill-designed to the task at hand. The lack of clarity or rigour behind those definitions means that there is a well-attested tendency for counter-terrorism operations to expand beyond the initially stated boundaries.

14. Counter-terrorism justifications have continued salience in dominant political discourse, demonstrated by the limited extent of confrontation with national definitions of terrorism and the necessity of exceptional powers in response. This has granted state agencies largely unchecked opportunities to intervene in citizens' lives so long as doing so is linked, in some way, to broad and self-defined counter-terrorism objectives.[21] Surveillance has become the natural means by which this intervention has been given effect, as it provides for extensive intervention in citizens' lives with limited chance of detection or public scrutiny.

15. While surveillance has taken many forms in counter-terrorism, contemporary scrutiny in this field focuses upon software which is capable of covert and undetected targeted intrusion and inspection of networks, computers, and devices. Such intrusion software allows access to fixed and mobile devices so that the content of users' communications, and other information including metadata (including location, duration, source and recipient of such communications) may be monitored covertly and remotely. These technological tools are typically known as 'spyware,' and referred to as such in this paper, although, given the covert nature and secret capacities of some of these tools, an exhaustive definition of features of spyware technology is not possible.

16. Spyware varies, and the covert nature of the products can mean that their operation is poorly understood even by regulators and users. These tools gain access to individual computers or mobile devices, with some programmes enticing the user to a communication seemingly from a known contact, and other programmes requiring no user action at all (known as an 'zero click' capability).[22] Once a device is infected, the spyware operators can typically

[21] A/76/261, [16]-[19].

[22] A/HRC/51/17, [7].

“

[I]f somebody can pay so much to control/monitor your communication, he’s ready to do much more. In time, they could put some information in my devices (my professional devices), and through that they can steal everything in my phone, they can record messages from themselves in my phone. I fear that.

”

- Placide Kayumba
Rwandan activist and member of the opposition in exile since 1994

Source: Access Now, ‘The Victims of NSO’s WhatsApp Hack’, 18 December 2020, https://www.accessnow.org/nso-whatsapp-hacking-victims-stories/

access and record video, audio, and text/email communications, including on supposedly secure platforms such as WhatsApp, as well as accessing calendars, contacts, and geolocation data. Spyware technology can also access other connected devices, such as wearable technological devices or vehicles, which may hold further data regarding health and location.[23] Moreover, spyware technology grants its user not only the ability to monitor targets, but also to manipulate the infected devices, including by altering, deleting, or adding files, which may be used for forgery or planting of incriminating data.[24]

17. While in previous eras, spycraft and surveillance technology tended to be the exclusive preserve of government agencies and in-house technical experts, in the modern era the vast majority of surveillance tools used by state agencies are obtained from the private sector. Private cyber-security firms responsible for tools with such capabilities include the Israel-based NSO,[25] Quadream,[26] and Candiru/Saito Tech,[27] the UK-based Gamma International Ltd, the German-based Vilicius Holding GmbH[28] and Trovicor GmbH, the France-basd Qosmos and Amesys, the Italy-based Area SpA[29] and Hacking Team/Memento Labs,[30] the firm Cytrox, which has divisions in North Macedonia, Israel and Hungary,[31] the US firms Cyberpoint, Narus (a Boeing subsidiary), BlueCoat Systems, and Cisco Sysems,[32] and the UAE firm Darkmatter.[33]

---

[23] A/HRC/51/17, [8].

[24] A/HRC/39/29, [19].

[25] AL OTH 211/2021 and AL/ISR 7/2021, though NSO has operations elsewhere also: see AL BGR 2/2021.

[26] See: G Megiddo, 'Secretive Israeli cyber firm selling spy-tech to Saudi Arabia,' Haaretz (8 June 2021), available at: https://www.haaretz.com/israel-news/tech-news/.premium.HIGHLIGHT-the-secret-israeli-cyber-firm-selling-spy-tech-to-saudia-arabia-1.9884403

[27] See: A Ziv, 'Top secret Israeli cyberattack firm revealed,' *Haaretz* (4 January 2019), available at: https://www.haaretz.com/middle-east-news/.premium-top-secret-israeli-cyberattack-firm-revealed-1.6805950

[28] Formerly FinFisher GmbH prior to restructuring following insolvency in December 2021. See: Open Corporates, Vilicius Holding GmbH, available at: https://opencorporates.com/companies/de/D2601V_HRB205476

[29] See: L Ferrarella, 'Assad intercettava gli oppositori al regime con tecnologia made in Italy,' *Corriere della Serra* (1 December 2016), available at: https://milano.corriere.it/notizie/cronaca/16_dicembre_01/assad-siria-intercettazioni-intercettava-oppositori-regime-tecnologia-made-italy-2420c69e-b7b1-11e6-a82f-f4dafb547583.shtml

[30] Hacking Team was acquired in 2019 by Memento Labs. See: P O'Neill, 'The fall and rise of a spyware empire,' *MIT Technology Review* (29 November 2019), available at: https://www.technologyreview.com/2019/11/29/131803/the-fall-and-rise-of-a-spyware-empire/

[31] See: B Marczak et al., 'Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware,' The Citizen Lab (16 December 2021), available at: https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

[32] See: European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, 'Pegasus and surveillance spyware,' May 2022, available at: https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf

[33] See: M Mazzetti and A Goldman, 'Ex-US intelligence officers admit to hacking crimes in work for Emiratis,' *The New York Times* (14 September 2021), available at: https://www.nytimes.com/2021/09/14/us/politics/darkmatter-uae-hacks.html

18. Civil society groups (among them Citizen Lab and Amnesty International) employing computer forensic analysis have identified commercial sophisticated spyware and surveillance technology developed by these firms being used by repressive State agencies worldwide. A worldwide media investigation led by the journalism non-profit organization Forbidden Stories considered leaked lists of 50,000 phone numbers potentially targeted by NSO's Pegasus software has linked the tool to the hacking of at least hundreds of smartphones, including family members of the murdered journalist Jamal Khashoggi,[34] senior politicians in Spain (including the Prime Minister, Defence Minister and more than 60 Catalan politicians, lawyers and activities),[35] the President of France, Mr Macron, and hundreds of other targets across countries including Bahrain, Saudi Arabia, Togo, the United Kingdom, and the United States comprising politicians, diplomats, journalists, human rights activists, and others.[36] In testimony before the European Parliament committee in June 2022, NSO revealed that Pegasus is used by States to target 12,000 to 13,000 individuals each year.[37] In addition, the FinFisher suite of tools has been implicated in hacking against Bahraini, Turkmen,[38] Ethiopian,[39] and Ugandan[40] targets among others. Further examples include Narus's technology being used in Egypt,[41] Trovicor's across the Middle East and North Africa,[42] and BlueCoat's in Iran, Sudan, and Syria.[43] In addition,

---

[34] R Bergman and P Kingsley, 'Israeli Spyware Maker Is in Spotlight Amid Reports of Wide Abuses,' *The New York Times* (18 July 2021), available at: https://www.nytimes.com/2021/07/18/world/middleeast/israel-nso-pegasus-spyware.html

[35] AL ESP 8/2022.

[36] A/HRC/51/17, [5]. AL ISR 11/2021.

[37] See: https://multimedia.europarl.europa.eu/en/webstreaming/pega-committee-meeting_20220621-1500-COMMITTEE-PEGA

[38] N Perlroth, 'Software Meant to Fight Crime Is Used to Spy on Dissidents,' *The New York Times* (30 August 2012), available at: https://www.nytimes.com/2012/08/31/technology/finspy-software-is-tracking-political-dissidents.html

[39] See the allegations in Doe v Federal Democratic Republic of Ethiopia, 851 F.3d 7 (D.C. Cir. 2017), as per the First Amended Complaint (18 July 2014); and Privacy International, 'Surveillance Follows Ethiopian Political Refugee to the UK' (16 February 2014), available at: https://privacyinternational.org/blog/1199/surveillance-follows-ethiopian-political-refugee-uk

[40] Privacy International, 'For God and My President: State Surveillance In Uganda' (October 2015), available at: https://privacyinternational.org/sites/default/files/2017-12/Uganda_Report_1.pdf

[41] T Karr, 'One US Corporation's Role in Egypt's Brutal Crackdown,' *Huffington Post* (28 January 2011), available at: https://www.huffpost.com/entry/one-us-corporations-role

[42] V Silver and B Elgin, 'Torture in Bahrain Becomes Routine with Help from Nokia Siemens,' *Bloomberg*, (22 August 2011), available at: https://www.bloomberg.com/news/articles/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking

[43] E Nakashima, 'Report: Web monitoring devices made by US firm Blue Coat detected in Iran, Sudan,' *The Washington Post* (8 July 2013), available at: https://www.washingtonpost.com/world/national-security/report-web-monitoring-devices-made-by-us-firm-blue-coat-detected-in-iran-sudan/2013/07/08/09877ad6-e7cf-11e2-a301-ea5a8116d211_story.html

investigations by the Citizen Lab and by the European Parliament's in-house technological experts have revealed that Cytrox's Predator spyware has been found on the devices of two prominent Egyptian figures (an exiled politician and a journalist) and a Greek Member of the European Parliament.[44]

19. Spyware is deployed worldwide by national security and law enforcement agencies in service of legitimate counter-terrorism and criminal investigative objectives. The Special Rapporteur recognizes that, as terrorism becomes increasingly sophisticated and itself entails ever-greater reliance upon digital technology and communications, it is unavoidable that government agencies will focus increasing resources upon technological surveillance tools which seek to keep up with, and outflank, those who pose a threat to national security and public safety.

20. But the general legitimacy of counter-terrorism and law enforcement objectives, and the imperatives for innovation created by the threat environment and the development of criminals' own technological capacity cannot justify a lack of due respect to fundamental human rights safeguards. Just as importantly, States must be mindful of the risk that the development of such technologies in the private sector, and their promulgation through trade and partnerships between States, raises risks of the transfer and dispersal of this technology to repressive environments, and into the hands of criminals as well as UN designated terrorist organizations.

21. The use of the tools outlined above is vulnerable to serious violations of international human rights law in various ways, including:

21.1. Violations of the right to life;[45]

---

[44] M Stevis-Gridneff and M Pronczuk, 'Senior European Parliament Member Targeted as Spyware Abuse Spreads' *The New York Times* (27 July 2022), available at: https://www.nytimes.com/2022/07/27/world/europe/eu-spyware-predator-pegasus.html

[45] UN General Assembly, International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 ('ICCPR'), Article 6(1).

21.2. Unlawful exposure to physical violence (including sexual violence),[46] unlawful arrest,[47] and/or harassment from government or private actors;

21.3. Disproportionate interference with individuals' right to privacy;[48]

21.4. Disproportionate interference with the rights to freedom of expression,[49] freedom of association,[50] and freedom of religion;[51]

21.5. The production and entrenchment of particular gender harms including direct harms to women and girls,[52] as well and LGBTQI+ persons;

21.6. Interference with the integrity of documentary records and evidence, undermining procedural fairness and the rule of law; and

21.7. Obstacles for individuals' ability to obtain effective remedies for breaches of their human rights.

[46] ICCPR, Article 7.

[47] ICCPR, Article 9.

[48] ICCPR, Article 17.

[49] ICCPR, Article 19.

[50] ICCPR, Article 22.

[51] ICCPR, Article 18.

[52] ICCPR, 2(1); ICESCR, Article 2(2); and CEDAW, Article 2.

Violations of the Right to Life / Exposure to Physical Risk

22. The development and trade of spyware tools poses substantial human rights risks due to the significant increases in the efficiency and precision of identifying, locating, and gathering personal information about target individuals. Spyware provides its users with the ability to observe and record a target's movements, communications, and actions (including in real time). That monitoring and evidence-gathering infrastructure allows for criminal investigative work to be conducted quickly and without detection, but it can equally facilitate persecution of target individuals, making them more easily subject to harassment, detention, and/or physical violence, even death.

23. The UN High Commissioner on Human Rights has noted there is a troubling weight of evidence that a variety of States may be deploying surveillance technology to identify and track individuals who are subsequently subject to arbitrary detention, unlawful violence, inhumane treatment, and even extrajudicial killings.[53] As the then UN Special Rapporteur on Extrajudicial, Summary, or Arbitrary Executions outlined in her 2019 investigation into the unlawful death of the journalist Jamal Khashoggi,[54] there is evidence that the mobile devices of the Saudi political activist Omar Abdulaziz, with whom Mr Khashoggi was in regular contact, had been infected with Pegasus spyware which was being operated in Saudi Arabia.[55] In ongoing legal proceedings brought in the Tel Aviv District Court against Pegasus's manufacturer NSO, Mr Abdulaziz alleges that Saudi authorities monitored his communications to gain intelligence against Mr Khashoggi prior to his murder in October 2018. An attempt by NSO to have the case struck out has failed.[56]

---

[53] See: A/HRC/41/35, [1]; and Committee on Legal Affairs and Human Rights, Parliamentary Assembly of the Council of Europe, Statement by UN High Commissioner for Human Rights (14 September 2021), available at: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27455&LangID=E

[54] UN Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Investigation into the Unlawful Death of Mr Jamal Khashoggi, UN Doc. A/HRC/41/CRP.1 (19 June 2019) ('Khashoggi Report').

[55] Khashoggi Report, [68]-[69].

[56] O Holmes and S Kirchgaessner, 'Israeli Spyware Firm Fails to Get Hacking Case Dismissed,' *The Guardian* (16 January 2020), available at: https://www.theguardian.com/world/2020/jan/16/israeli-spyware-firm-nso-hacking-case

“In any case, it is exactly like being undressed by someone in public, stripped naked, and you are powerless before an invisible hand and a terrifying faceless force.”

- Father Pierre Marie-Chanel Affognon
Togolese Catholic priest and founder of the movement to promote constitutional, institutional, and electoral reform in Togo

Source: Access Now, ‘The Victims of NSO’s WhatsApp Hack’, 18 December 2020, https://www.accessnow.org/nso-whatsapp-hacking-victims-stories/

24. Forensic digital investigations by the University of Toronto's Citizen Lab and the Ireland-based NGO Front Line Defenders also indicate that a number of Bahraini dissidents subjected to torture, including the journalist Yusuf al-Jamri and the human rights defender Ms Ebtisam Al-Saegh, had been subject to long-term surveillance by the Bahraini National Security Agency ('NSA') using Pegasus.[57] Ms. Al-Saegh has given accounts of her treatment at the hands of NSA officials in 2017, alleging that she was immediately blindfolded when taken into custody, and then beaten and sexually assaulted.[58] But the evidence of continued targeting is ten years after the claimed reform of the NSA following the Bahrain Independent Commission of Inquiry, established by the government in answer to the torture and death in NSA custody of businessman Karim Al-Fakhrawi.[59] Further, in June 2021, executives of the French cybersurveillance manufacturers Amesys and Nexa Technologies were indicted for complicity in torture allegedly carried out by the Libyan and Egyptian authorities against political dissidents.[60] Most recently, in August 2022, the English High Court concluded that a Saudi dissident Mr Ghanem Al-Masarir was monitored via Pegasus spyware operated by the Saudi authorities, and was assaulted in London by persons answerable to those authorities.[61] These individual cases illustrate the gravity and systematic nature of the human rights violations that are implicated by the use of spyware in multiple national contexts.

25. Further, there is evidence that spyware tools designed for counter-terrorism surveillance by governments are being misused in private settings, facilitating gender-based violence through stalking, coercive control, and gender-based harassment both online and off.[62] Authorities are capable of weaponizing the information they

---

[57] B Marczak et al., 'From Pearl to Pegasus: Bahraini Government Hacks Activists with NSO Group Zero-Click iPhone Exploits,' Citizen Lab, University of Toronto (24 August 2021), available at: https://citizenlab.ca/2021/08/bahrain-hacks-activists-with-nso-group-zero-click-iphone-exploits/

[58] See: P Beaumont, 'Activist who accused Bahrain security forces of sexual assault is rearrested,' *The Guardian* (6 July 2017), available at: https://www.theguardian.com/world/2017/jul/06/activist-rearrested-bahrain-risk-torture-amnesty-international-ebtisam-al-saegh

[59] Bahrain Independent Commission of Inquiry, 'Report of the Bahrain Independent Commission of Inquiry' (10 December 2011), available at: https://www.bici.org.bh/BICIreportEN.pdf

[60] P Samama, 'Cybersurveillance en Libye: La Société Française Amesys Mise en Examen pour "Complicité d'Actes de Torture,"' *BFM Business* (1 July 2021), available at: https://www.bfmtv.com/economie/entreprises/cybersurveillance-en-libye-la-societe-francaise-amesys-mise-en-examen-pour-complicite-d-actes-de-torture_AD-202107010312.html; and Fédération Internationale pour les Droits Humains, 'Surveillance et Torture en Egypte et en Libya - Des Dirigeants d'Amesys et Nexa Technologies Mis en Examen' (22 June 2021), available at: https://www.fidh.org/fr/regions/maghreb-moyen-orient/egypte/surveillance-et-torture-en-egypte-et-en-libye-des-dirigeants-d-amesys

[61] Al-Masarir v Kingdom of Saudi Arabia [2022] EWHC 2199 (QB), [191] (Knowles J).

[62] In addition to the gendered impacts of State surveillance itself, which has particular effects along gender lines as set out in detail in the recent report, 'Human rights impact of counter-terrorism and countering (violent) extremism policies and practices on the rights of women, girls and the family,' UN Doc. A/HRC/46/36 (22 January 2021), [11]-[12].

extract through campaigns of gender-based defamation, blackmail (often through the threatened publication of private images), or doxxing.[63] In 2021, the English High Court accepted evidence that NSO Pegasus tools had been used in the context of a dispute between HRH Mohammed bin Rashid Al Maktoum, the Prime Minister of the UAE, and his former wife HRH Princess Haya bint Al Hussein, about the welfare of their two children,[64] with the Princess and her lawyer targeted. NSO identified the use, notified the Princess's representatives, and within hours modified the technology so that it could no longer be used against UK-registered mobile phone numbers (the technology is also not designed to be capable of targeting mobile devices registered in the US, Canada, Australia, or New Zealand).[65]

26. Freedom from physical harm in its various forms is among the most basic internationally-accepted principles of human rights. All persons have the right to life,[66] to freedom from arbitrary detention,[67] and to freedom from torture, and from cruel, inhuman or degrading treatment or punishment.[68] These rights are non-derogable, meaning that States must comply with them even in exceptional circumstances of public emergency[69] or armed conflict.[70]

27. States may be implicated in various ways in the use of spyware which puts the lives and security of targets in danger from those who would do them harm. Of course, repressive regimes which deliberately use spyware as an instrument to facilitate threats to life and unlawful treatment will formally be liable directly for the violation of victims' human rights. That is the case even where the technical operation of the spyware system is – as is often the case – effectively sub-contracted to technical expert teams in the private sector, typically through aftermarket support staff provided by the same corporations providing the technology in the first place. But further, States allowing the development of spyware technology within their jurisdictions and authorizing its trade and transfer both domestically and across borders into the hands of public authorities

---

[63] As noted in: M Fatafta, 'Unsafe anywhere: women human rights defenders speak out about Pegasus attacks,' *Access Now* (17 January 2022), available at: https://www.accessnow.org/women-human-rights-defenders-pegasus-attacks-bahrain-jordan/

[64] See the judgment in: Re Al M [2021] EWHC 1162 (Fam).

[65] D Sabbagh, 'NSO Pegasus spyware can no longer target UK phone numbers,' *The Guardian* (8 October 2021), available at: https://www.theguardian.com/world/2021/oct/08/nso-pegasus-spyware-can-no-longer-target-uk-phone-numbers.

[66] ICCPR, Article 6(1).

[67] ICCPR, Article 9. While the right to liberty and security of the person is not included in the list of non-derogable rights in Article 4(2), the aspect of the right relating to freedom from arbitrary detention is non-derogable, even in public emergency situations. See: UN Human Rights Committee, *General Comment 35*, UN Doc. CCPR/C/GC/35 (16 December 2014), [65].

or private purchasers abroad are also charged with specific legal obligations as a matter of international human rights law.

28. First, that is because a State's obligation to avoid violations of human rights includes an obligation to carry out some degree of due diligence to prevent violations by third parties. The UN Human Rights Committee – the specialist expert body tasked with providing authoritative guidance on the interpretation of the human rights standards set out in the ICCPR – has stated in its General Comment 36 on the Right to Life, that States must exercise '*due diligence to protect the lives of individuals against deprivations caused by persons or entities whose conduct is not attributable to the State.*'[71] This involves taking '*special measures of protection towards persons in vulnerable situations whose lives have been placed at particular risk because of specific threats or pre-existing patterns of violence*' including '*human rights defenders, officials fighting corruption and organized crime, humanitarian workers, journalists, prominent public figures, witnesses to crime and victims of domestic and gender-based violence and human trafficking.*'[72]

29. The obligations upon States to respect and protect human life go further still. As General Comment 36 observes: '*States parties must take appropriate measures to protect individuals against deprivation of life by other States, international organizations and foreign corporations operating within their or in other areas subject to their jurisdiction. They must also take appropriate legislative and other measures to ensure that all activities taking place in whole or in part within their territory and in other places subject to their jurisdiction, but having a direct and reasonably foreseeable impact on the right to life of individuals outside their territory, including activities taken by corporate entities based in their territory or subject to their jurisdiction, are consistent with [ICCPR] article 6, taking due account of related international standards of corporate responsibility, and the right of victims to obtain an effectively remedy.*'[73]

---

[68] ICCPR, Article 7. See also: UN General Assembly, Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (adopted 10 December 1984, entered into force 26 June 1987) 1465 UNTS 85, Article 2(1).

[69] ICCPR, Article 4(2).

[70] UN Human Rights Committee, General Comment 36, UN Doc. CCPR/C/GC/36 (3 September 2019) ('General Comment 36'), [2]. See also: UN Human Rights Committee, General Comment 6, UN Doc. HRI/GEN/1/Rev.1 at 6 (1994), [1].

[71] General Comment 36, [7].

[72] General Comment 36, [23].

[73] General Comment 36, [22].

30. While State obligations in international human rights law are tied to the State's jurisdiction (originally understood as simply coterminous with the State's physical territory), it is now accepted that a State exercises jurisdiction outside its territory whenever the State has (a) *effective control* over an extra-territorial area or (b) exercises authority and control over individuals (wherever located).[74]

31. The boundaries of what amounts to exercising authority and control over individuals are not conclusively settled, but a growing number of international legal experts argue that this arises whenever the State has, on the facts of a particular case, the capacity to affect an individual's enjoyment of rights (wherever that individual is located).[75] As noted by Judge Bonello of the Grand Chamber of the European Court of Human Rights in his separate concurring opinion in the European Court case of Al-Skeini v UK:

> *'10. States ensure the observance of human rights in five primordial ways: firstly, by not violating (through their agents) human rights; secondly by having in place systems which prevent breaches of human rights; thirdly, by investigating complaints of human rights abuses; fourthly, by scourging those of their agents who infringe human rights; and finally, by compensating the victims of breach of human rights ...*
>
> *11. ...Very simply put, a State has jurisdiction [and thus responsibility for breaches] whenever the observance or the breach of these functions is within its authority and control.'* [76]

32. The Special Rapporteur has previously endorsed this view of extraterritorial jurisdiction in her amicus curiae brief before the European Court of Human Rights in the case of HF v France concerning the obligations of France in respect of French nationals in North East Syria.[77] The Special Rapporteur on extrajudicial, summary or arbitrary executions has also explicitly endorsed this approach to jurisdiction in her report on the investigation

---

[74] See: Georgia v Russia (II) [2021] ECHR 58; (2021) 73 EHRR 6 (GC), [113]-[115].

[75] Notably Prof Yuvan Shany, who was, together with Sir Nigel Rodley, co-author of the draft of General Comment 36. See: Y Shany, 'Taking Universality Seriously: A Functional Approach to Extraterritoriality in International Human Rights Law' (2013) 7 The Law & Ethics of Human Rights 47.

[76] Al-Skeini v United Kingdom [2011] ECHR 1093; (2011) 53 EHRR 18 (GC), Concurring Opinion of Judge Bonello, [10]-[11].

[77] HF and ors v France [2022] ECHR 678 (GC), [179].

into the unlawful death of Jamal Khashoggi, concluding that a State's responsibility to protect the right to life '*may be invoked extra-territorially in circumstances where the particular State has the capacities to protect the right to life on an individuals against an immediate or foreseeable threat to his or her life.*'[78] The Federal Constitutional Court of Germany has similarly concluded that State agencies are responsible for the extraterritorial human rights implications of digital surveillance against targets abroad.[79]

33. Separately, it is generally agreed that international law recognizes the liability of a State where it 'aids or assists' another State in the commission of an internationally wrongful act. Article 16 of the International Law Commission's Draft Articles on State Responsibility provides that '*A State which aids or assists another State in the commission of an internationally wrongful act by the latter is internationally responsible for doing so if: (a) that State does so with knowledge of the circumstances of the internationally wrongful act; and (b) the act would be internationally wrongful if committed by that State.*'[80] This principle of liability for *aiding or assisting* another State's violations of international law has been recognized as reflecting customary international law by, *inter alios*, the International Court of Justice in the *Bosnia Genocide* decision,[81] and in domestic litigation before the Federal Constitutional Court of Germany,[82] and the UK courts.[83]

34. Consequently, States using spyware to identify targets for violence, harassment, and abuse, and to arm agents with details to locate and persecute those targets, whether at home or abroad, may violate targets' rights to life, and their entitlement to freedom from arbitrary detention, torture, or cruel or inhuman treatment or punishment. Further, States facilitating or turning a blind eye to the production and export, from their own territory, of spyware to foreign regimes carrying out such violations may also give rise to responsibility where a State fails to take sufficient steps to prevent those human rights breaches.

---

78 Annex to the Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions. Investigation into the unlawful death of Mr Jamal Khashoggi, UN Doc. A/HRC/C/41/CRP.1 (19 June 2019), [360]. See to analogous effect the decisions of the Committee on the Rights of the Child in Saatchi v Argentina, UN Doc. CRC/C/88/D/104/2019 (8 October 2021).

79 BVerfG, *Judgment of the First Senate of 19 May 2020*, 1 BvR 2835/17.

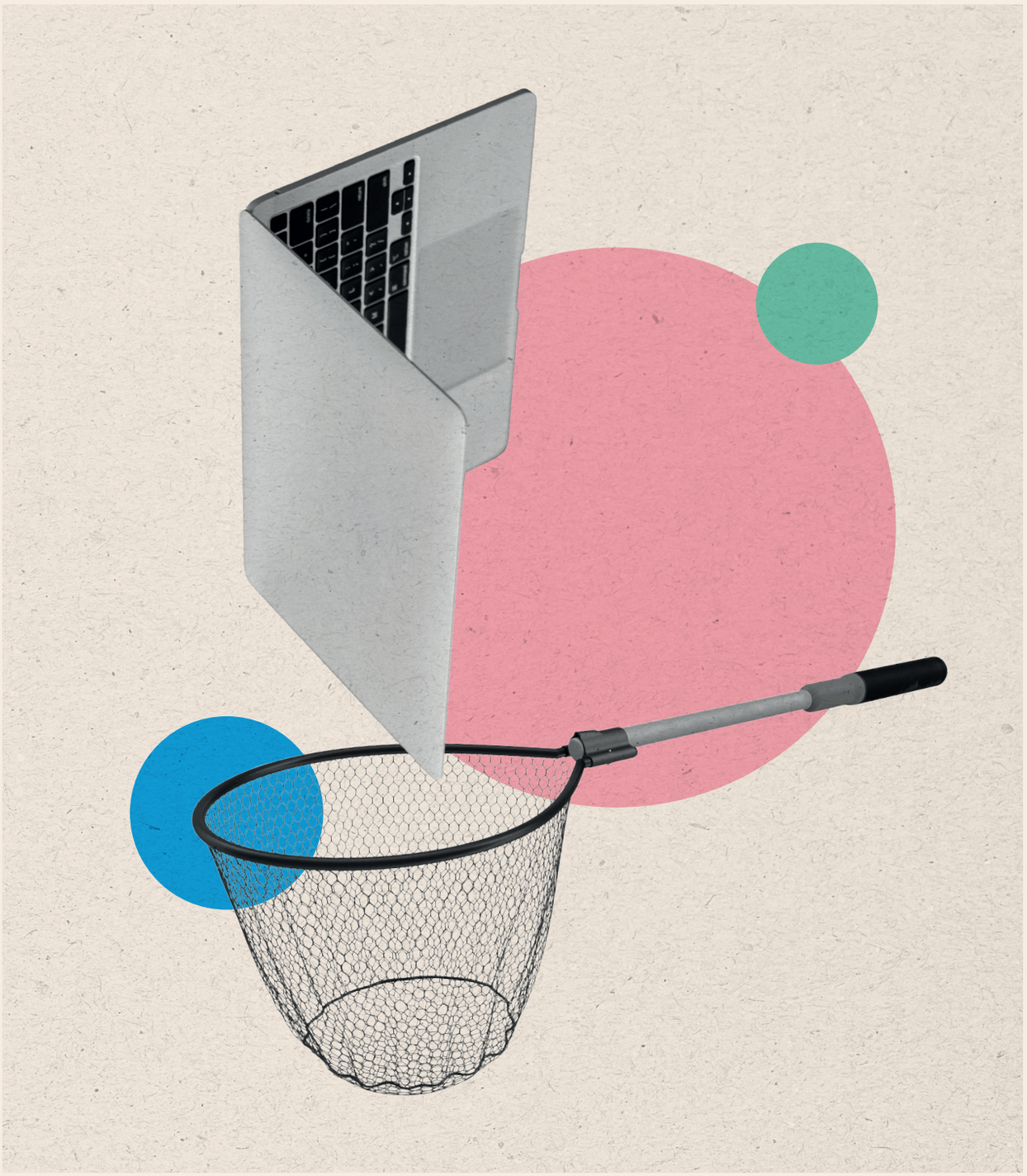
80 UN General Assembly Resolution No 56/83 on the Responsibility of States for Internationally Wrongful Acts, UN Doc. A/RES/56/83 (28 January 2002). See also, International Law Commission, 'Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries,' available at: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf

81 See: *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Servia and Montenegro)*, Judgment of 26 February 2007, ICJ Rep 2007, p42, [420]. See also the dissenting opinion of Judge Schwebel in *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States)*, ICJ Rep 1986, p14, [558].

82 *Al-M* (5 November 2003) 2 BVerfG 1506/03, [54].

83 *R (Al-Saadoon) v Secretary of State for Defence* [2015] 3 WLR 503 (Admin), [193] (Leggatt J).

35. The risk posed to individual targets of ill-treatment including summary or arbitrary execution by powerful cyber surveillance tools, including spyware, which provide State agencies with precise location details and evidence of what those targets are saying and doing is clear, and enlivens the obligations of States under international law.



“It’s every journalist who has been targeted’s concern that once it’s revealed that you were surveilled and even our confidential messages could have been compromised, who the hell is going to talk to us in the future?... Everyone will think that we’re toxic, that we’re a liability.”

- Szabolcs Panyi
Investigative journalist (Direkt6)
Hungary

Source: Phineas Rueckert, ‘NSO’s Pegasus: The Israeli Cyber Weapon Oppressive Regimes Used Against 180 Journalists,’ *Haaretz* (18 July 2021), https://www.haaretz.com/israel-news/tech-news/2021-07-18/ty-article/.premium/nsos-pegasus-the-israeli-cyber-weapon-used-against-180-journalists/0000017f-dc8d-df62-a9ff-dcdfe86d0000

Disproportionate Interference with Privacy

36. Setting aside cases where surveillance leads to physical harm, the use of surveillance technology in counter-terrorism programmes by its nature has potential impacts on the right to privacy. Under international human rights law, every person enjoys the right to private and family life without undue interference,[84] with that protection extending to their digital communications.[85] The Special Rapporteur underscores the significance of the right to privacy as a 'gateway' right, a right which is essential to the protection and promotion of other rights, specifically those rights considered non-derogable under international law.

37. Both the General Assembly and the Human Rights Council have stressed that the right to privacy serves as one of the foundations of democratic societies and, as such, plays an important role in the realization of a host of other rights, including the rights to freedom of opinion and expression, freedom of religion, and free assembly and association.[86] But given the interconnected nature of human rights, the adverse impacts of privacy violations may entail more widespread rights infringements, including upon the right to equal protection of the law, the right to life, the right to liberty and security of the person, the rights to fair trial and due process, the right to freedom of movement, the right to enjoy the highest attainable standard of health, and the right to have access to work and social security. [87]

38. As the then UN High Commissioner for Human Rights observed in her ground-breaking 2014 report on 'The Right to Privacy in the Digital Age,' both the content of communications and their metadata are protected by the right to privacy, since even metadata may reveal insights into

---

[84] ICCPR, Article 17.

[85] Human rights bodies have taken an expansive view on what comes within the scope of privacy protection in the context of digital information, including: audio-visual surveillance (*El Haski v Belgium* [2012] ECHR 2019; (2013) 56 EHRR 31, [102]; metadata (Malone v United Kingdom [1984] ECHR 10; (1985) 7 EHRR 14, [84]); and geolocation information (*Uzun v Germany* [2010] ECHR 2263; (2011) 53 EHRR 24, [12]-[13]).

[86] A/RES/71/199; A/RES/73/179; A/HRC/RES/34/7.

[87] As set out in the Special Rapporteur's report 'Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?' (University of Minnesota Human Rights Center, 2020).

individual's behaviour and allow conclusions to be drawn about their private lives.[88] Interferences with the right to privacy are only permissible in limited circumstances where they not only serve a legitimate objective,[89] but are strictly necessary and proportionate in their effect. In this regard, governments frequently justify digital surveillance programmes which interfere with rights to privacy on the grounds of counter-terrorism objectives. The pursuit of such objectives is clearly capable of qualifying as a legitimate aim for the purposes of an assessment of human rights compliance, but the degree of interference must be considered in light of the necessity of the measure to achieve the aim and the actual benefit it yields.[90] In another context,[91] the HRC has clarified that such consideration requires that the infringement is the 'least intrusive instrument amongst those which might achieve their protective functions,'[92] and has counselled that, '[i]n adopting laws providing for restrictions permitted [for legitimate aims], States should always be guided by the principle that the restrictions must not impair the essence of the right … the relation between the right and restriction, between norm and exception, must not be reversed. The laws authorising the application of restrictions should use precise criteria and may not confer unfettered discretion on those charged with heir execution.'[93]

39. Much previous human rights criticism of digital surveillance programmes has focused on the frequently overbroad nature of such programmes.[94] The human rights concerns posed by spyware are typically of a different type as spyware is specifically targeted (at least at the level of the subject, although the degree of information collected about that person and their contacts may still be disproportionate and overbroad).[95]

---

[88] A/HRC/27/37 (30 June 2014)), [19].

[89] Article 17 of the ICCPR does not expressly set out that interferences may be justified on the basis of a legitimate objective, but the consistent approach of the Human Rights Committee, in common with regional human rights courts, is to read that implied limitation into the scope of the right. See, for instance: HRC, *Van Hulst v Netherlands*, UN Doc. CCPR/C/82/D/903/1999 (2004), [7.6]-[7.10]; and *Weber and Saravia v Germany* (App No. 54934/00), Decision of 29 June 2006, [103]-[137].

[90] A/HRC/27/37, [24].

[91] The right to freedom of movement under ICCPR, Article 12.

[92] HRC, *General Comment 27*, UN Doc. CCPR/C/21/Rev.1/Add/9 (1999), [14]; and HRC, *General Comment 34*, UN Doc. CCPR/C/GC/34 (2011), [34].

[93] HRC, *General Comment 27*, [13].

[94] See, for instance, the repeated declarations that bulk surveillance programs are inconsistent with the right to privacy in: A/69/397 (23 September 2014); UN Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression and Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Joint Declaration on Surveillance Programs and their Impact on Freedom of Expression (21 June 2013); Court of Justice of the European Union in Case C-362/14 *Schrems v Data Protection Commissioner* ECLI:EU:C:20-15:650; and the European Court of Human Rights, most recently in *Big Brother Watch and ors v United Kingdom* [2021] ECHR 439 (GC).

[95] As noted by Prof Kaye, 'Here's what world leaders must do about spyware,' above n 16.

40. **But specificity of targeting will not render it lawful when the spyware collects all information about a person and their contacts, going beyond what may be relevant for investigative purposes.** Further, where it is generally the case spyware is employed at the arbitrary discretion of State agencies without proper legislative authority or oversight or used in service of illegitimate aims such as the persecution of political opponents, or disproportionate to any legitimate criminal or security objective. In the recent example[96] of the Pegasus spyware infection of the devices of Princess Latifa of Dubai, who alleges that she was kidnapped and imprisoned after trying to leave the country, and her supporter Mr David Haigh, if such targeting were to have been carried out under State instigation (which has been denied by the UAE), there would appear to be no lawful basis for the acts involved. There is no suggestion that Princess Latifa is the target of any legitimate investigation or suspicion,[97] or for that matter that Mr Haigh would be a legitimate target merely as a result of his raising awareness of her apparent disappearance and calling for evidence of her safety and whereabouts.

41. Further, the Special Rapporteur asserts that even if there were some internal justification for surveillance held by a particular State agency, the pervasive secrecy and lack of oversight governing the deployment of such tools raises serious questions as to how such surveillance can possibly comply with the fundamental legal requirements as to the existence of legislative authority or the guarantee that the interference with rights imposed by the surveillance is strictly confined to what is necessary and proportionate for its stated aims.[98] The complexity of these tools, the operations of which are specifically designed to avoid detection and analysis, pose unique challenges to oversight and accountability.

42. The threat of spyware use to privacy is particularly acute given the counter-terrorism context, because one of the typical legislative backstops against privacy infringement – a data protection regime – is typically ousted by domestic counter-terrorism

---

[96] See: 'Pegasus: Princess Latifa and Princess Haya numbers "among leaks,"' *BBC News* (21 July 2021), available at: https://www.bbc.co.uk/news/world-middle-east-57922543; and D Sabbagh, 'Princess Latifa campaigner had "phone compromised by Pegasus spyware,"' *The Guardian* (2 August 2021), available at: https://www.theguardian.com/world/2021/aug/02/princess-latifa-campaigner-david-haigh-phone-compromised-pegasus-spyware

[97] Some international human rights jurisprudence suggests that, alongside or as part of considerations of necessity and proportionality, targeted surveillance may only be lawful where there exists a 'reasonable suspicion' that the target of the surveillance has committed or is likely to commit criminal acts. See: *Roman Zakharov v Russia* [2015] ECHR 1065 (GC), [260]-[263]; and *Big Brother Watch v United Kingdom* [2021] ECHR 439 (GC), Separate Opinion of Judge Pinto de Albuquerque, [24].

[98] It would be preferable for States to obtain prior judicial authorization for spyware surveillance, as noted by the Special Rapporteur on the freedom of opinion and expression at A/HRC/41/35, [52]. Such a process is unlikely to be adopted by the regimes which rely upon spyware for repressive purposes.

legislation. Data protection regimes grant data subjects the opportunity to obtain and, where appropriate, correct or request removal of, inaccurate or inappropriately-held personal information. For instance, the EU's governing data protection framework – the General Data Protection Regulation[99] – does not apply to data processing by law enforcement and criminal justice authorities, and even the weaker data processing rules which do (the so-called Law Enforcement Directive)[100] do not regulate data collection, retention, processing, and/or sharing where this occurs for national security purposes.

43. While the Pegasus leaks are the most recent example, the monitoring with spyware of individuals who do not appear to present any plausible terror or criminal threat has been well-attested for at least a decade. The US-based Ethiopian democracy activist known pseudonymously as Mr Kidane brought proceedings in US Federal court[101] following a forensic investigation establishing that his computer devices had been infected with FinSpy tools which were transmitting private data to the servers of Ethio Telecom (the Ethiopian state-owned telecommunications company).[102] Analysis revealed that, between October 2012 and March 2013, the FinSpy software installed on Mr Kidane's devices made audio recordings of his Skype calls, recorded the contents of emails, and the results of web searches (including apparently for school projects carried out by Mr Kidane's children). The developer of the FinSpy suite of tools – Gamma International – maintains it only provides the technology to State agency customers, but the responsibility of the Ethiopian authorities has never been established. But whatever the entity responsible, it is difficult to conceive how intrusive technology targeting a democracy activist which covertly transfers such a wide swathe of information to the operator could fall within the boundaries of a lawfully-authorized, proportionate response to a pressing legitimate criminal investigative aim.

44. Finally with respect of privacy impacts, the Special Rapporteur

---

[99] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4 May 2016, pp1-88.

[100] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4 May 2016, pp89-131.

[101] *Doe v Federal Democratic Republic of Ethiopia* 851 F.3d 7 (DC Cir. 2017).

[102] For a summary of the case, see: 'Case Note: Doe v Federal Democratic Republic of Ethiopia' (2018) 131 *Harvard Law Review* 1179.

sets out her deep concern that the inherent capacities of spyware which allows for absolute control over the entirety of a subject's digital life may render it impossible for uses of the technology to comply with the requirements that any surveillance be limited to what is necessary and proportionate to any purported legitimate aim. If certain spyware technology harvests and records all data and metadata for a device without any capacity for discrimination or limitation by the user, this appears prima facie incompatible with human rights, since there would be no operational capacity for the type of limitation required of human rights compliance.[103] As Professor Kaye, the former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has observed:

> *'Analog surveillance tools, such as the wiretapping of a fixed line telephone or mobile phone, typically enables access to conversations – itself a potential problem but not the vast access to one's contacts, location data, keystrokes, video and so on. It is containable in its aim both by judicial warrant and technology. Spyware like Pegasus, by contrast, may not be so limiting. Its intrusiveness is difficult to constrain. In legal terms, it may be difficult if not impossible for a state to demonstrate its use of spyware for narrow purposes and without "collaterally" sweeping in personal data having no relevance to a legitimate governmental purpose.'*[104]

45. If, therefore, a particular type of spyware is structured in such a manner as to, for instance, automatically obtain and record all data and metadata from a device, denying its user the opportunity to limit its interference to what may strictly be necessary and proportionate, **it appears unlikely that any regulatory system could prevent the use of such spyware from being unlawful**. If, by its inherent operation, a certain spyware technology necessarily accesses data which goes beyond which is legitimately necessary and proportionate for the purposes of criminal or counter-terrorism investigation, and if, in particular, spyware automatically harvests extensive data including contact details of people who are not the targets of the investigation in which the technology is deployed, **it would appear inevitable that such spyware is incapable of human rights compliance, at least until that technology is redesigned and its capabilities restricted**.

---

[103] The former Special Rapporteur on freedom of opinion and expression considered that the lack of convincing evidence that the use of spyware technologies can be technically restricted to lawful purposes justified a moratorium: A/HRC/41/35, [49].

[104] D Kaye, 'The Spyware State and the Prospects for Accountability,' (2021) 27(4) *Global Governance* 483-492, p492.

46. A regulatory response to spyware will, therefore, only be appropriate insofar as spyware technology is engineered in a manner allowing for limitations to be placed upon the extent of its interference with targets' privacy. **In the Special Rapporteur's view there may well, however, be a category of spyware which, by virtue of indiscriminate and disproportionate impacts, can never be operated in a lawful manner and which must therefore be subject to a comprehensive ban, whatever may be the approach for less-intrusive technology.**

Disproportionate Interference with Freedom of Expression, Peaceful Assembly, Association, and Religion

47. Given that surveillance tools are deployed in respect of digital communications channels (principally the Internet and telecommunication) used for transfer of information, fundraising, and organizing of individuals, such deployment has clear implications for individuals' use of those communication channels, and thus their rights to freedom of expression, which includes the right both to impart and to receive[105] information without undue restriction. Freedom of expression is also protected worldwide as a fundamental right,[106] and should be considered of particular importance, since it provides the mechanism by which other rights, such as political participation,[107] freedom of peaceful assembly[108] and association,[109] and freedom of religion or belief,[110] may be exercised. As the HRC put it in its *General Comment 34*:

> *'Freedom of opinion and freedom of expression are indispensable conditions for the full development of the person. They are essential for any society. They constitute the foundation stone for every free and democratic society … Freedom of expression is a necessary condition for the realization of the principles of transparency and accountability that are, in turn, essential for the promotion and protection of human rights.'*[111]

48. The right applies broadly, and includes '*political discourse, commentary on one's own and public affairs, canvassing, discussion of human rights, journalism, cultural and artistic expression, teaching and religious discourse.*'[112] Further, as regional courts have made clear, opinion and expression does not lose its protection merely by virtue of being untrue, shocking, offensive, or disturbing, or indeed by challenging the democratic principles upon which its protection is justified.[113] If interferences with the exercise of free

---

[105] As specifically noted by the Grand Chamber of the European Court of Human Rights: *Magyar Helsinki Bizottság* [2016] ECHR 975, [165].

[106] ICCPR, Article 19.

[107] See: HRC, *Gauthier v Canada*, UN Doc. CCPR/C/65/D/633/1995, [13.4]; and *Aduayom, Diasso and Dobou v Togo*, UN Doc. CCPRC/57/D/422-4/1990, [7.4].

[108] ICCPR, Article 21.

[109] ICCPR, Article 22.

[110] ICCPR, Article 18.

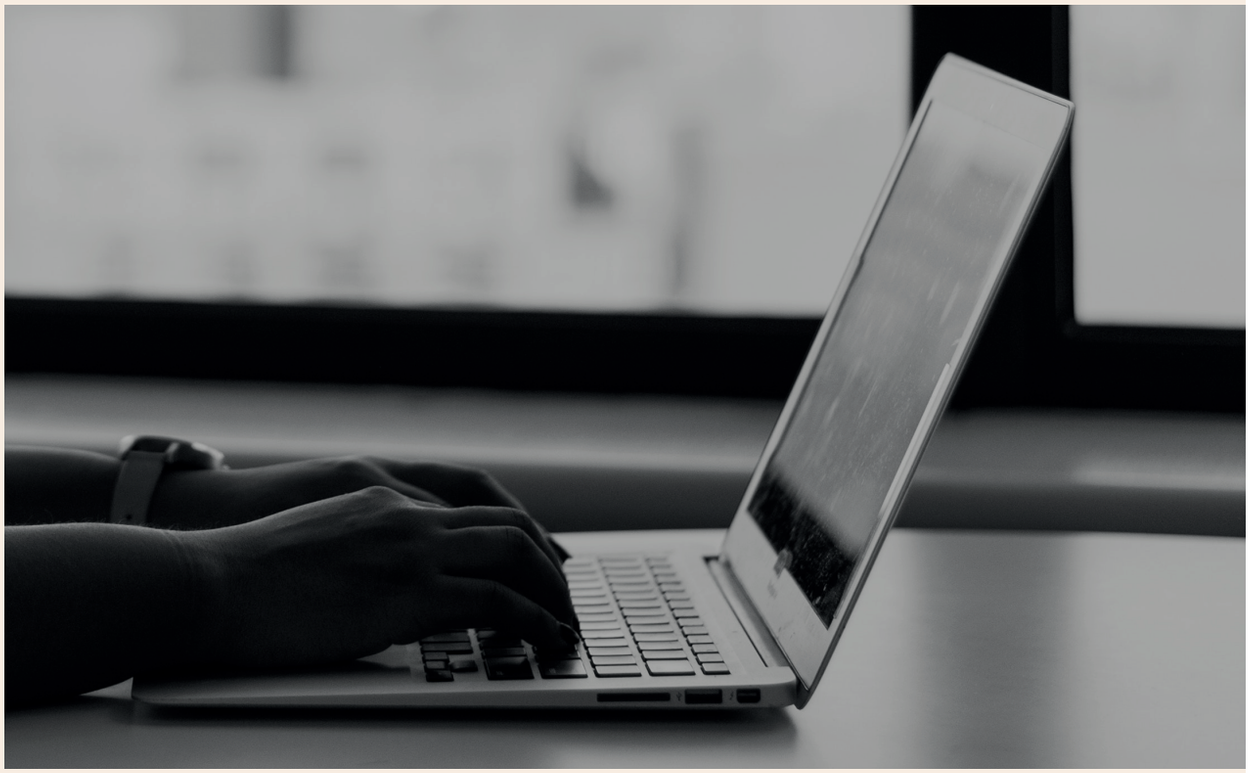
[111] HRC, *General Comment 34*, UN Doc. CCPR/C/GC/34 (12 September 2011), [2].

[112] *General Comment 34*, [11].

[113] *Handyside v United Kingdom* [1975] ECHR 5; (1976) 1 EHRR 737, [49]; and Gündüz v Turkey [2003] ECHR 652, [51].

expression and related rights are to be lawful, they must be non-arbitrary, must pursue a closed list of legitimate aims, and the effect of the restriction must be no more than is necessary and proportionate to achieve the aim.[114] Free expression rights are most at issue when individuals seek to express minority or controversial opinions. Accordingly, States need to be particularly alive to the risks of infringement posed by a counter-terrorism framework which restricts statements which are alleged to incite, encourage, glorify, or support terrorism or violent extremism conducive to terrorism (as counter-terrorism legislation worldwide frequently does).

49. The interferences with expression and ancillary rights represented by the use of spyware tools are obvious[115] and come in many forms. First, as the UN



[114] HRC, *General Comment 27*, [14]; and HRC, *General Comment 34*, [34].

[115] Council of Europe, Information Society Department, 'Pegasus Spyware and its impacts on human rights,' DGI(2022)04.

High Commissioner for Human Rights has made clear, the very existence of digital surveillance creates interferences with rights,[116] since the knowledge of such surveillance risks, and the desire to avoid targeting from them, leads citizens to change their behaviour, alter and limit the manner in which they express themselves and communicate with others, and in effect self-censor.[117] Due to this 'chilling effect,' surveillance technology affects not only those persons whose data is actually collected, but also those whose data is never obtained because of the threat of violations. The chilling effect is all the more acute in the case of concerns about spyware due to the fact that not only targets, but all contacts, are potentially affected by the such tools.[118]

50. This concern is particularly keenly felt by persons already targeted by State authorities, such as representatives of religious, ethnic, gender or sexual minorities, members of certain political parties or trade unions, human rights defenders, and professionals such as lawyers and journalists.[119] As the former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression recently put it, the '*very possibility*' of spyware surveillance presents knock-on impacts on civil society and democratic discourse since it '*would likely serve to deter journalists from working on the most sensitive sorts of topics, not to mention the willingness of sources and whistleblowers to come forward to reporters.*'[120] Prominent examples of repressive regimes' use of spyware have entailed the targeting of activists, lawyers, and journalists.[121] In the words of the Supreme Court of India in its recent decision on Pegasus, the chilling effect of spyware represents an 'assault on the vital public watchdog role of the press.'[122] Unchecked proliferation of spyware technology can be expected to lead to further targeting of dissident voices and, through the fear of such ubiquitous scrutiny, disincentivize civic participation by all citizens. As the Greek MEP Nikos Androulakis put it following revelations that his mobile devices had been hacked (by an unknown actor) with the Predator spyware: '*Revealing who's behind these appalling practices and who they are acting for isn't a personal matter, it's a democratic duty.*'[123]

---

[116] A/HRC/27/37, [20].

[117] See: A/HRC/32/38, [57].

[118] A/HRC/51/17, [12].

[119] A/HRC/32/38, [57]. See also: A/HRC/29/32.

[120] Kaye, above n 104, 489.

[121] See the examples collated by the Committee for the Protection of Journalists, 'Special report: When spyware turns phones into weapons,' 13 October 2022, available at: https://cpj.org/reports/2022/10/when-spyware-turns-phones-into-weapons/

[122] Supreme Court of India, *Manohar Lal Sharma v Union of India*, Order of 27 October 2021, [39].

[123] M Stevis-Gridneff and M Pronczuk, above n 44.

“The hacking of my phone played a major role in what happened to Jamal [Khashoggi], I am really sorry to say, the guilt is killing me.”

- Omar Abdulaziz
Saudi Arabian Activist in exile in Canada
Runs a satirical news show on YouTube reporting on Saudi Government

Source: Abdualaziz told CNN in 2018, reported in Suzan Quitaz, “Pegasus; The Israeli spyware that helped Saudi Arabia spy on Khashoggi”, *The New Arab* (3 October 2019), https://english.alaraby.co.uk/analysis/israeli-spyware-helped-saudi-arabia-spy-khashoggi.

Gender Harms

51. The human rights risks set out above arise regardless of gender, but gender may exacerbate those risks. It is accepted that gendered harm may be experienced by men and by women, but the specific aspects of spyware misuse on women's human rights are particularly noteworthy. Women may be at particular risk of violence, invasion of privacy, and interferences with free expression and civil participation linked to spyware. For instance, human rights defenders, dissidents, and journalists of all genders have been subject of, and are at risk of, targeting with spyware and the violence and threats to which such targeting can give rise. But women in such roles are particular targets of misogynist abuse, sexual harassment (including through the non-consensual dissemination of sexualized or intimate images (real or fake)), and intimidation (including through threatened of actual 'doxxing' – that is, the publication online of real world contact and/or location details).[124] UNESCO research suggests that women journalists are particularly exposed to online attacks,[125] and the gender-specific and often sexualized nature of such intimidation has been described by the Special Rapporteur on violence against women as '*a direct attack on women's visibility and full participation in public life.*'[126] Given that spyware allows not only for harvesting and publication of real data, but also the alteration and faking of data for potential use in blackmail, doxxing, and intimidation, the concern is even more pronounced than with other modes of surveillance.

52. The targets of Pegasus spyware have included prominent women's rights campaigners in Bahrain and Jordan,[127] as well as, it is suspected, dozens of female activists, journalists, and others across the Middle East, North Africa, and India. As the Internet Freedom Foundation has noted, the targeting of women's devices with spyware may be '*different from a man being targeted because any information can always be used to blackmail or discredit her*' via actual or threatened exposure of real or fake sexualized content.[128] Spyware provides a perfectly-designed mechanism to

---

[124] See: Report of the UN Special Rapporteur on Violence Against Women, Its Causes and Consequences on Online Violence Against Women and Girls from a Human Rights Perspective, UN Doc. A/HRC/38/47, [30]-[42].

[125] UNESCO, 'World Trends in Freedom of Expression and Media Development: Global Report 2021/2022,' pp97-99. See also: UNESCO, 'The Chilling: Global Trends in Online Violence Against Women Journalists' (April 2021).

[126] A/HRC/38/47, [29].

[127] S Kirchgaessner, 'Two female activitists in Bahrain and Jordan hacked with NSO spyware,' *The Guardian* (17 January 2022), available at: https://www.theguardian.com/news/2022/jan/17/two-female-activists-in-bahrain-and-jordan-hacked-with-nso-spyware

[128] R Chandran and M Gebeily, 'Pegasus spyware has put women in the global south at risk of blackmail, harassment and even "bodily harm," experts and victims say,' *Reuters* (11 August 2021), available at: https://news.trust.org/item/20210811000007-hlyz7/

arm the perpetrators of gender-based threats and intimidation with the weapons they use to silence female voices in civic society. As such, the existence and deployment of spyware must be assumed to have an outsized impact in chilling women's freedom of expression, freedom of association, and ability to participate meaningfully in public life.

53. But in addition to women being particularly at risk of the sorts of violations of privacy and fundamental freedoms which may affect all targets of spyware technology, the use of spyware against women also gives rise to separate violations of specific protections for women contained in international human rights law.

54. To start with, the right to freedom of discriminatory treatment on the grounds of gender is set out in all major human rights treaties.[129] Such treatment takes many forms, and, as the Committee on the Elimination of Discrimination Against Women ('CEDAW Committee') has observed, includes gender-based violence. Gender-based violence means any violence '*that is directed against a woman because she is a women or that affects women disproportionately. It includes acts that inflict physical, mental or sexual harm or suffering, threats of such acts, coercion and other deprivations of liberty.*'[130] States are thus required, pursuant to their obligations to avoid direct or indirect discrimination,[131] to refrain from any actions which (whether intentionally or otherwise) facilitate gender-based violence, and to take appropriate steps to address it. Insofar as States facilitate – directly or indirectly – the targeting of women with actual or threatened gender-based physical violence, then such States are failing to uphold their obligations with respect to non-discrimination on gender grounds.

55. Further, while the use of spyware against prominent female activists is a matter of substantial concern, it likely represents only a fraction of the gender-based violence associated with spyware technology. The proliferation of such technology out of official hands and into the public at large raises pronounced risks of increased intimate partner violence. There is a considerable degree of evidence that data covertly harvested from devices are misused for coercive control[132] and in stalking/harassment,[133] with a significant increase in such violations in recent years.[134] While complicated by their positions as royal and thus political figures, the use of spyware to target HRH Princess Latifa and HRH Princess Haya of the UAE during periods of actual or alleged family

---

[129] ICCPR, 2(1); ICESCR, Article 2(2); and CEDAW, Article 2.

[130] CEDAW Committee, General Recommendation 19, UN Doc. A/47/38 at 1 (1992), [6].

[131] Indirect discrimination occurring whenever a measure is neutral at face value but nonetheless has the '*purpose or effect*' of impairing women's enjoyment of their rights and freedoms. See: HRC, *General Comment 18*, UN Doc. HRI/GEN/1/Rev.1 at 26 (1994), [7]; and HRC, Althammer v Austria, UN Doc. CCPR/C/78/D/998/2001, [10.2].

[132] See, for instance: B Harris and D Woodlock, 'Digital Coercive Control: Insights from Two Landmark Domestic Violence Studies' (2019) 59(3) *British Journal of Criminology* 530; D Woodlock et al., 'Technology as a Weapon in Domestic Violence: Responding to Digital Coercive Control' (2019) 73(3) Australian Social Work 1.

[133] D Freed et al., '"A Stalker's Paradise:" How Intimate Partner Abusers Exploit Technology,' (2018) *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* 1-13.

[134] Research suggests that digital stalking activity increased dramatically after the imposition of the Covid-19 lockdowns. See: Interpol, 'Taking a Stand Against Online Stalking' (21 April 2021), available at: https://www.interpol.int/en/News-and-Events/News/2021/Taking-a-stand-against-online-stalking

dispute is a reminder that coercive control may be found in all sectors of society.

56. Human rights law also imposes a series of specific obligations aimed at advancing women's formal and substantive equality. Article 3 of CEDAW, for instance, provides that:

> *'States Parties shall take in all fields, in particular in the political, social, economic and cultural fields, all appropriate measures, including legislation, to ensure the full development and advancement of women, for the purpose of guaranteeing them the exercise and enjoyment of human rights and fundamental freedoms on a basis of equality with men.'* [135]

57. The language of Article 3 is mandatory ('*shall take*') and expansive ('*in all fields … all appropriate measures*'), making it clear that CEDAW obligations require immediate implementation across the board, rather than progressive realization.[136] The reference to '*all fields*' is especially significant. It '*anticipates the emergence of new forms of discrimination that had not been identified at the time of [CEDAW's] drafting,*'[137] and makes clear that States' obligations apply across the board.

58. As interpreted by the CEDAW Committee, Article 3 implies a series of duties for States. The Committee's General Recommendation 25, which draws upon the language of Article 3, set out that '*States Parties to the Convention are under a legal obligation to respect, protect, promote and fulfil this right to non-discrimination for women and to ensure the development and advancement of women in order to improve their position to one of de jure as well as de facto equality with men.*'[138] Accordingly, States are under an obligation to exercise due

---

[135] See also, ICCPR, Article 3: '*The States Parties to the present Covenant undertake to ensure the equal right of men and women to the enjoyment of all civil and political rights set forth in the present Covenant.*'

[136] Cf. ICESCR, Article 2(1).

[137] CEDAW Committee, *General Recommendation 28*, UN Doc. CEDAW/C/GC/28 (2010), [8].

[138] CEDAW Committee, *General Recommendation 25*, UN Doc. HRI/GEN/1/Rev.7 at 282 (2004), [4]. See also CEDAW Committee, General Recommendation 28, [16].

diligence in fields under their control to take steps to prevent women's advancement and development being impeded by non-State actors, including by violence or threats of violence, whether from State agents or private parties. That obligation has been made clear in CEDAW Committee's approach to the State's obligation of due diligence where women are at risk of intimate partner violence, as set out in the cases of *Sahide Goecke v Austria*[139] and *Yildirim v Austria*.[140]

59. The risks that the use of spyware even by private parties poses for women, who may be more readily exposed to violence and/or coercion in relation to actual or threatened exposure of private – often sexualized – information, are, as a matter of international law and specifically affirmed by the Special Rapporteur, something which State agencies must actively have in mind and guard against. **Decisions to allow spyware use or spyware export approvals are obliged to be accompanied with robust due diligence strategies to minimize the potential for gender harms arising from this powerful and invasive technology, and robust record-keeping and audit functions so that misuse can be efficiently investigated, evidenced, and remedied. These audit functions ought to include some mechanism of digital watermarking such that spyware can ultimately be linked to its producer and their governmental client, with the result that avenues of remedy (against producer or governmental user) can be accessed.**

---

[138] CEDAW Committee, *General Recommendation 25*, UN Doc. HRI/GEN/1/Rev.7 at 282 (2004), [4]. See also CEDAW Committee, General Recommendation 28, [16].

[139] CEDAW Committee, *Sahidi Goecke v Austria*, UN Doc. CEDAW/C/39/D/5/2005 (2007), [12.1.6].

[140] CEDAW Committee, *Yildirim v Austria*, UN Doc. CEDAW/C/39/D/6/2005 (2007), [3.1]. See also the conclusions on the deaths of multiple women in Ciudad Juárez in: CEDAW Committee, Report on Mexico produced by the Committee on the Elimination of Discrimination Against Women under art 8 of the Optional Protocol to the Convention, and reply from the Government of Mexico, UN Doc. CEDAW/C/2005/OP.8/MEXICO, [50].

[141] *General Comment 32*, UN Doc. CCPR/C/GC/32 (23 August 2007), [13].

[142] A/HRC/23/40, [62].

Impact on Fair Trial and Due Process

60. The right to a fair trial is a fundamental guarantee of human rights and the rule of law. It contains various interrelated aspects and is often linked to the enjoyment of other rights, such as the right to life and the prohibition against torture and other forms of cruel, inhuman or degrading treatment or punishment. Article 14 of the ICCPR provides that, '*[i]n the determination of any criminal charge against suit at law, everyone shall be entitled to a fair and public hearing by a competent, independent and impartial tribunal established by law.*' The same fundamental principle of fairness applies in all proceedings, including civil and administrative matters.

61. As the Human Rights Committee has observed in *General Comment 32*, the operation of a fair hearing requires, inter alia, that all parties to a dispute have a real opportunity to contest all arguments and evidence.[141] That in turn requires that such evidence is accurate and has not been subject to interference or manipulation, something which, given the power imbalances between individual accused persons and State investigative and prosecutorial bodies, is the obligation of the State to guarantee.

62. But, as the UN Special Rapporteur on the freedom of expression has noted with regard to government hacking, the risk exists that, as part of digital intrusion, there may occur alterations to targets' digital records. Spyware allows for '*a new for[m] of surveillance*' which opens the door to third parties (be they State agencies or other actors) '*alter[ing] – inadvertently or purposefully – the information contained therein,' which in turn 'threatens not only the right to privacy [but also] procedural fairness rights with respect to the use of such evidence in legal proceedings.'*[142]

63. In the Special Rapporteur's view any uncertainty as to the integrity of the evidential record of investigations based upon spyware-enabled investigation would be catastrophic across multiple bases. Not only would it constitute violations of the entitlements of the accused to fair trials in their own cases, but it would also jeopardize the safety of any convictions, casting doubt on

---

[141] *General Comment 32*, UN Doc. CCPR/C/GC/32 (23 August 2007), [13].

[142] A/HRC/23/40, [62].

the integrity of proceedings and potentially undermining all legitimate investigations infected with such methods. As the OHCHR noted in the 2022 'Right to Privacy in the Digital Age' report, spyware tools allow unscrupulous users '*to forge evidence in order to incriminate or blackmail targeted individuals.*'[143]

64. In light of these risks, the Special Rapporteur takes the view that spyware technology which allows for alterations to data without any record or account of such alterations presents such a threat to fair trial rights that it is unlikely that such technology could ever be used in a manner compliant with international human rights law. A fair hearing depends upon the integrity of evidence, such that technology capable of altering evidence covertly and without an audit trail showing what alterations have been made, when, and by whom, is inimical to a fair hearing. The effort to introduce a more robust regulatory system is not intended to obscure the fact that there may well be types of spyware with certain capacities which are incapable of being operated lawfully, and thus have no place in any regulated system of international development and trade.

65. Just as a fair hearing depends upon the integrity of the evidence, so too it depends upon the sanctity of the privileged communications between persons subject to the jurisdiction of a tribunal and their legal advisers and representatives. Article 14(3)(b) of the ICCPR guarantees the right of an accused person to communicate with their legal counsel. The Human Rights Committee has long made clear that Article 14 will be violated if the privacy of such legally privileged communications is not maintained.[144] Limitations upon the privacy of legally privileged communications have also been held incompatible with fair trial rights by the European Court of Human Rights.[145] Very specific derogations from the privacy of such communications might theoretically be acceptable if there is a specific risk of, for instance, conspiracy between the legal representative, the accused, and criminals who remain at large, but as a previous holder of this mandate has set out, '*[w]here measures are taken to monitor the conduct of consultations between legal counsel and client, strict procedures must be established to ensure that there can be no deliberate or inadvertent use of information subject to legal professional privilege. Due to the importance of the role of counsel in a*

[143] A/HRC/51/17, [11].

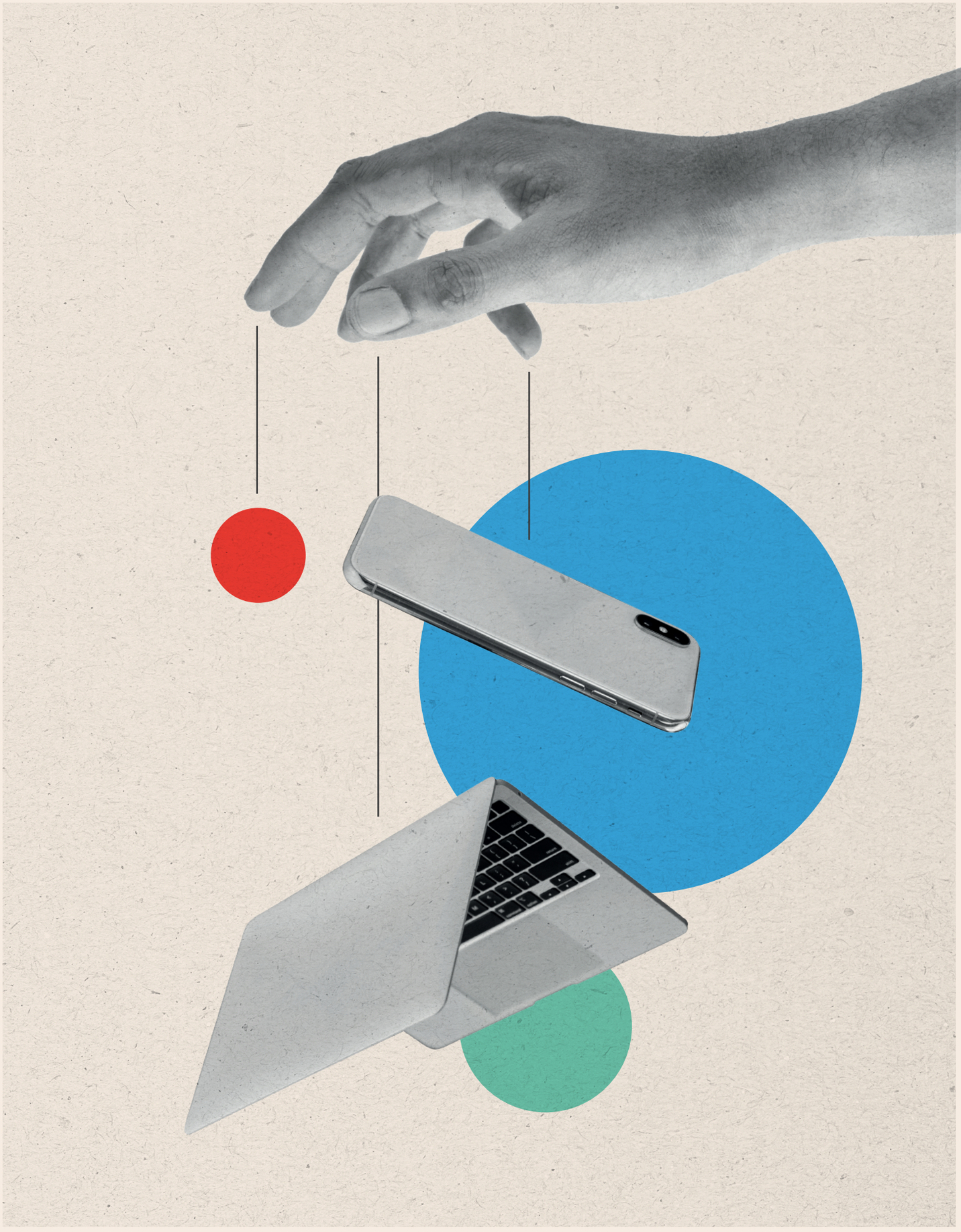
[144] *Khomidova v Tajikistan*, UN Doc. CCPR/C/81/D/1117/2002 (29 July 2004), [6.4]; *Gridin v Russian Federation*, UN Doc. CCPR/C/69/D/770/1997 (18 July 2000), [8.5]; and Sigareva and Sigarev v Uzbekistan, UN Doc. CCPR/C/85/D/907/2000 (1 November 2005), [6.3].

[145] *Brennan v United Kingdom* [2001] ECHR 596; (2002) 34 EHRR 18, [59]-[63].

fair hearing, and of the chilling effect upon the solicitor-client relationship that could follow the monitoring of conversations, such monitoring should be used rarely and only when exceptional circumstances justify this in a specific case.' [146]

66. **In the Special Rapporteur's view, if spyware technology is incapable of discrimination, such that all data including the contents of legally privileged communications is necessarily and automatically monitored and recorded, especially if there is no audit record of such activity, then it follows that such technology cannot be deployed in a manner which is compatible, even in theory, with the restrictions imposed by human rights law.** If a spyware tool allows users to access, record, alter, delete and/or manipulate a target's data and there is no indelible and non-editable audit trail or record of what the user has done such that there can be proper oversight and review after the fact, then the spyware tool is incapable of being used in a manner which is compliant with basic standards of due process and fair trial, all of which depends upon integrity of evidence. Such spyware technology, so long as it retains the technical capacity to carry out operations without any permanent auditable record of the same, cannot exist in compliance with international human rights law. Again, the result of this may be that, for any lawful development and trade in spyware technology to be contemplated, and any regulation to be considered, it first needs to be made clear that the capacities of spyware technology must observe certain basic limits as to the capacity of the technology to be targeted (rather than indiscriminate) and its capacity to have its operations recorded (rather than obscured from review). **Only once any such tool is re-engineered to provide for an adequate permanent record-keeping function is there the prospect of a regulated, human-rights compliant function for the technology.**

[146] A/63/223, [39].



Impact on Effective Remedies

67. The right of all individuals to effective remedies for any breaches of their rights is also a fundamental principle of international human rights law.[147] The field of surveillance by State agencies poses challenges for conventional structures of accountability and redress. The element of cross-border transfers of technology presents particular jurisdictional and/or practical obstacles. Additionally, because of the role private actors play in developing and/or operating technology there are limitations to the remedies available for rights breaches. Human rights law imposes obligations to make available effective remedies to people whose rights have been violated. This 'right to a remedy' has often been identified as one of the central aspects of an effective framework for human rights protection.[148] The HRC has emphasized that, even in times of emergency, States must comply with the 'fundamental obligation … to provide a remedy that is effective.'[149] For remedies to be 'effective,' they must satisfy the criteria of being: prompt;[150] practical rather than theoretical;[151] determined by an independent authority;[152] and accessible (without undue practical or financial barriers).[153]

68. In this respect, breaches of human rights involving the use of surveillance technology in the counter-terrorism context present real difficulties. First, as a matter of jurisdiction, States have often created a separate judicial architecture (typically so-called 'secret courts') governing cases involving national security matters, which display departures from ordinary rules regarding access to evidence, secrecy of proceedings, or appeal arrangements.[154]

69. In addition to the limitations on remedies within the counter-terrorism context per se, the technology itself creates specific challenges for access to effective remedies. Intrusive surveillance technology may be employed by State authorities through partnership with, or co-option of, privately-operated communications networks (with or without those operators' knowledge).[155] This may complicate access to justice, as judicial remedies addressing a paradigm of direct State exertion of public power over

---

[154] For instance, so-called 'secret courts' operating in a number of jurisdictions and criticized by the European Court of Human Rights in *Al-Nashif v Bulgaria* [2002] ECHR 502; (2002) 36 EHRR 655.

[155] A/HRC/35/22, [17].

[156] A/RES/68/167 (21 January 2014).

individuals are poorly adapted to situations involving private network intermediaries. Further, the nature of modern communications networks, which operate worldwide and route communications traffic across national borders, create challenges for conventional legal remedial frameworks based on territorial jurisdiction.

70. While the UN General Assembly and the Human Rights Council, in the preambles to their 2013,[156] 2018,[157] and 2019[158] resolutions on the Right to Privacy in the Digital Age, have emphasized that extraterritorial surveillance enlivens State responsibility just as domestic surveillance does, the boundaries of extraterritorial State responsibility for digital surveillance are yet to be firmly established in international law. As noted above, recent human rights jurisprudence[159] shows movement away from the rigid historical model of jurisdiction over rights only arising where a State has physical authority over persons or effective control of foreign territory, and towards a more 'functional' model[160] whereby State agencies should be held responsible wherever their actions have the ability actually to affect individual rights, wherever those effects take place. But in the absence of a worldwide consensus of settled law holding States responsible for the impact of extraterritorial surveillance policies, affected individuals have little certainty that they will be able to vindicate their rights before national or regional courts.

71. In addition, there is the practical obstacle that the use by States of surveillance technologies is often concealed as a matter of fact and, even if revealed through leaks, goes unacknowledged. This means that affected individuals affected have minimal access to the evidence necessary to present their cases before competent tribunals.

---

[157] A/RES/73/179.

[158] A/HRC/RES/42/15.

[159] See, for instance: *Hanan v Germany* [2021] ECHR 131 (GC), [134]-[145]; *HF and ors v France* [2022] ECHR 678 (GC); and *Al-Skeini and ors v United Kingdom* [2011] ECHR 1093 (GC); (2011) 53 EHRR 18, Concurring Opinion of Judge Bonello, [10]-[13].

[160] As outlined in the HRC's *General Comment 36*, [63].

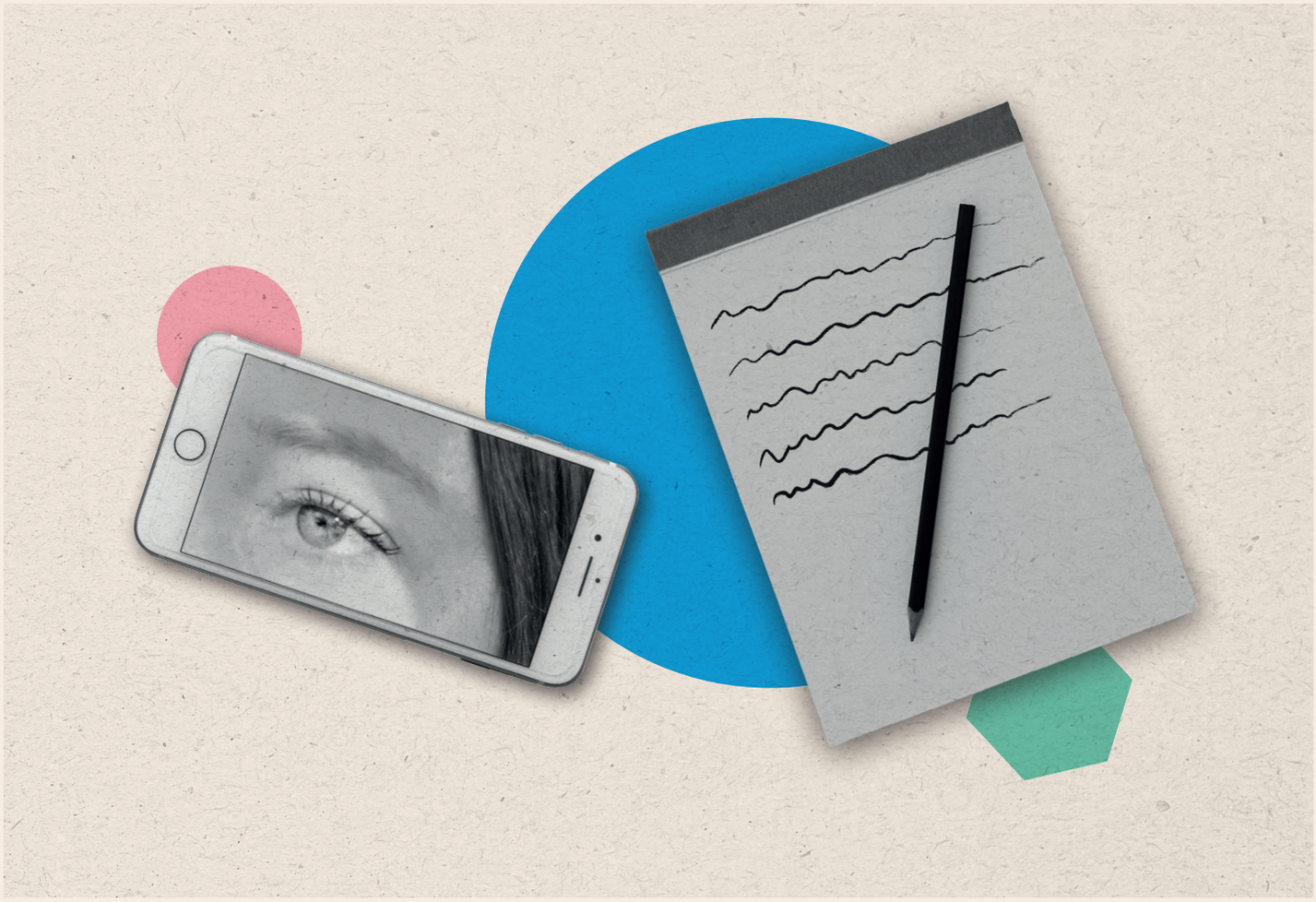
“

The monitoring of an MEP is illegal & unconstitutional. I will fight up to the end in revealing the truth and I will not allow any shadows in my life.

”

- Leader of the socialist opposition party PASOK (Greece’s third largest party) Member of the European Parliament

Source: Ugo Realfonzo, ‘Extent of Greek government spying scandal revealed at European Parliament inquiry,’ *The Brussels Times* (11 September 2022), https://www.brusselstimes.com/287632/extent-of-greek-government-spying-scandal-revealed-at-european-parliament-inquiry



04 Part II: Current Regulatory Frameworks Relevant to the Trade in Surveillance Technology

72. In the Special Rapporteur's view, given the substantial risk that the misuse of surveillance technology designed for counter-terrorism and law enforcement represents for human rights protection, businesses which manufacture that technology, States which allow that manufacture and the trade in that technology worldwide, and States which deploy that technology must all share responsibility for ensuring that risks are minimized and international human rights law is respected. A range of frameworks currently attempt to give effect to this straightforward principle, with varying degrees of success.

Regulation of Businesses Engaged in Surveillance Technology Industry

73. First of all, considering businesses which develop and supply surveillance technology, the framework regulating their actions comprises:

73.1. Their direct obligations – currently set out in non-binding 'soft law' principles of general agreement – to promote and protect international human rights, and their own policies (if any) giving effect to such obligations; and

73.2. Their domestic legal obligations under specific statutory requirements imposed upon their trade, or pursuant to general legal principles with which human rights obligations may be analogized.

74. As a matter of orthodox international human rights law, private parties do not themselves owe primary legal obligations to protect human rights and fundamental freedoms, since such obligations under the ICCPR[161] and other human rights conventions attach to State authorities alone. In some limited contexts, private industries have adopted voluntary industry standards which nod towards addressing human rights concerns,[162] but no such effort has been undertaken by the spyware technology industry.

---

[161] ICCPR, Article 2(1).

[162] See, in the context of private military and security contractors: the Montreux Document on Pertinent International Legal Obligations and Good Practices for States related to Operations of Private Military and Security Companies during Armed Conflict (2008); the International Code of Conduct for Private Security Service Providers (2010); and the ISO Standard 18788: Management system for private security operations (2015). See: Kaye, above n 104, 491.

75. The potentially-relevant 'soft law' instrument is the United Nations Guiding Principles on Business and Human Rights,[163] based upon a study mandated by the Secretary-General[164] and subsequently endorsed by the Human Rights Council in 2011.[165] These Guiding Principles propose that, quite apart from legal obligation, there is a normative '*global standard of expected conduct for all business enterprises*'[166] which requires that '*business enterprises should respect human rights … they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved.*'[167] That normative obligation is said to exist independent of any requirements imposed by national laws and regulations regarding human rights compliance.[168]

76. The Guiding Principles urge businesses, in giving effect to this normative obligation, to, among other things, conduct due diligence processes[169] that '*identify, prevent, mitigate and account for*' actual and potential human rights impacts,[170] and provide remedies wherever they have caused or contributed to adverse human rights impacts.[171] The High Commissioner for Human Rights has specifically urged businesses in the communications and digital technology sector to adopt explicit policies to secure compliance with the Guiding Principles, warning that where '*a company provides mass surveillance technology or equipment to States without adequate safeguards in place or where the information is otherwise used in violation of human rights, that company risks being complicit in or otherwise involved in human rights abuses.*' [172] The former Special Rapporteur on freedom of opinion and expression has urged surveillance companies to meet their Guiding Principles responsibilities through, at a minimum, adopting policies which foreground due diligence in client selection, require client compliance with human rights, prohibit product customization or targeting in violation of human rights by clients, engineer human

---

[163] Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, 'Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework,' UN Doc. A/HRC/17/31 (21 March 2011), Annex ('Ruggie Principles').

[164] The mandate was set out in: UN Commission on Human Rights, *Human Rights Resolution 2005/69*, UN Doc. E/CN.4/RES/2005/69 (20 April 2005).

[165] UN Human Rights Council, Resolution 17/4, UN Doc. A/HRC/RES/17/4 (16 June 2011).

[166] Ruggie Principles, Principle 11, Commentary.

[167] Ruggie Principles, Principle 11.

[168] Ruggie Principles, Principle 11, Commentary.

[169] The potential for confusion between legal and business definitions of 'due diligence' has been noted in: J Bonnitcha and R McCorquodale, 'The Concept of "Due Diligence" in the UN Guiding Principles on Business and Human Rights,' 2017) 28(3) *European Journal of International Law* 899.

[170] Ruggie Principles, Principle 17.

[171] Ruggie Principles, Principle 22.

[172] A/HRC/27/37, [43].

rights safeguards into products such as notification systems and 'kill switches' in circumstances of misuse, transparently report and periodically audit risks and cases of human rights harms, and
establish grievance and remedial mechanisms including compensation for individuals affected by misuse of surveillance products. [173]

77. The Guiding Principles have gained a significant status and have been incorporated in a range of international regulatory instruments which reiterate the importance of responsible corporate behaviour.[174] Further, they generally enjoy the support of civil society,[175] and work is currently ongoing to ensure better practical application of the standards set out for the activities of technology companies, with the OHCHR currently conducting a consultation on that topic.[176]

78. The Special Rapporteur is however deeply concerned there is no binding worldwide mechanism to ensure compliance with the Guiding Principles. Work is underway at the international level to negotiate an international legally-binding treaty on transnational corporations and other business enterprises with respect to human rights. Following the establishment of an open-ended working group by the UN Human Rights Council in 2014, a series of drafts for a treaty have been developed, most recently the Third Revised Draft following the 7th session of the working group in October 2021.[177] The basic obligations contemplated in the proposed treaty are that States parties must (a) protect individual victims of unlawful interferences with human rights committed by or through private entities, (b) prevent such unlawful interferences through the identification of actual and potential human rights abuses which may arise from business activities and take legal and policy measures to avoid the same, and (c) provide adequate and effective judicial and non-judicial remedies for human rights

---

[173] A/HRC/41/35, [60] and [67].

[174] See: Organisation for Economic Co-operation and Development (OECD), 'Guidelines for Multinational Enterprises' (2011) ('OECD Guidelines'), available at: https://www.oecd.org/daf/inv/mne/48004323.pdf; International Finance Corporation, 'Sustainability Performance Standards' (1 January 2012), available at: https://www.ifc.org/wps/wcm/connect/24e6bfc3-5de3-444d-be9b-226188c95454/PS_English_2012_Full-Document.pdf?MOD=AJPERES&CVID=jkV-X6h; and Equator Principles on Project Finance Requirements (July 2020), available at: https://equator-principles.com/app/uploads/The-Equator-Principles_EP4_July2020.pdf

[175] See: Human Rights Council, Panel Discussion on the Tenth Anniversary of the Guiding Principles on Business and Human Rights, Conference Room Paper, UN Doc. A/HRC/49/CRP.3 (10 February 2022), [31]-[35].

[176] See: https://www.ohchr.org/EN/Issues/Business/Pages/consultation-ungps-tech-companies.aspx

[177] Available at: https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/WGTransCorp/Session6/LBI3rdDRAFT.pdf

breaches involving businesses.[178] The negotiations on a binding treaty in this field suggest that international momentum is building towards the agreement of a potential mechanism.

79. The fact that the most recent round of negotiations included representation and active involvement from a number of international actors not previously engaged in the process (including the European Union, the United States, Japan, the United Kingdom, and Israel) has been welcomed by proponents of the binding treaty effort. The scope of the project, however, poses a substantial challenge to agreement on matters of detail. The proposed treaty, according to the Third Revised Draft, intends to provide an architecture to establish and codify the responsibilities of transnational corporations and States across all major international human rights treaties, including on an extraterritorial basis, all at once. But the notion of a single international standard of corporate responsibility for each human right is very ambitious, especially given the framing of some rights, particularly economic, social, and cultural rights like 'an adequate standard of living,' 'the highest attainable standard of physical and mental health,' and enjoyment of 'the benefits of scientific progress and its applications.' However, much progress has been made by those committed to a binding treaty on business and human rights, the scale of the project and the potential for differences of opinion is likely to mean that any concluded instrument is a long way off.

80. In the foreseeable future the closest thing to an agreed and implemented international approach to regulating businesses' impacts on human rights is the oversight architecture relating to the OECD Guidelines for Multinational Enterprises ('the OECD Guidelines'), a set of corporate responsibility guidelines relating to matters including human rights, employment and industrial relations, environment, bribery, consumer protection, competition, and taxation. With respect to human rights, the current version of the OECD Guidelines (revised in 2011) expressly cross-refer to the Guiding Principles and reflect their substance.[179] Under the OECD Guidelines, which have been adopted by 38 OECD member and 12 non-OECD adhering governments,[180] governments are obliged to establish

---

[178] See Articles 5, 6, and 7 of the Third Revised Draft.

[179] See: OECD Guidelines, pp31-34.

[180] See: https://mneguidelines.oecd.org/oecddeclarationanddecisions.htm

non-judicial grievance mechanisms known as National Contact Points for Responsible Business Conduct ('NCPs'), the role of which is to receive complaints regarding alleged non-compliance by business enterprises with, among other things, their human rights responsibilities. Of course, the system applies only to businesses registered in the participating group of countries, but a substantial majority of surveillance technology companies fall within that scope. Across the more than 20 years of the NCP grievance system, the caseload has been relatively modest[181] (an average of less than one case per country per year, albeit that the United States of America and United Kingdom NCPs have a caseload more than double that rate, receiving respectively 48 and 56 cases since 2000).[182]

81. The complaints brought under the OECD Guidelines framework have predominantly been concerned with environmental protection and with labour rights. The human rights cases have tended to relate to sales of arms. Within the NCP caseload, it appears that only three cases have been brought in respect of the potential adverse human rights impacts of businesses involved in the surveillance industry. Two cases were brought in parallel in 2013 by privacy and human rights NGOs[183] to the German and United Kingdom NCPs concerning the conduct of the companies Trovicor GmbH ('Trovicor') and Gamma International UK Ltd ('Gamma'). The complaints alleged that those companies had exported intrusive surveillance technology in the form of DPI tools and spyware to the Bahraini authorities, which were used for unlawful surveillance leading to breaches of privacy and free expression rights of the human rights activists Ala'a Shehabi, Husain Abdulla, and Shehab Hashem and the arbitrary arrest and torture of the activist Abdul Ghani Al-Khanjar.

82. In the case submitted to the German NCP, Trovicor refused to confirm whether it had supplied technology to the Bahraini regime, citing commercial confidentiality. Since the NGOs that brought the complaint did not have sight of the contractual arrangements, and the NCP had no power to compel Trovicor to disclose those arrangements, the NCP terminated the case without further action.[184] In the case submitted to the United Kingdom NCP,[185] Gamma similarly refused to confirm whether or not

---

[181] OECD, 'National Contact Points for Responsible Business Conduct: Providing Access to Remedy, 20 Years and the Road Ahead' (2020) ('NCP 20 Year Review'), available at: http://mneguidelines.oecd.org/NCPs-for-RBC-providing-access-to-remedy-20-years-and-the-road-ahead.pdf

[182] NCP 20 Year Review, pp61-62.

[183] The complaint to the German NCP was brought by: The European Center for Constitutional and Human Rights, Reporters without Borders, Bahrain Center for Human Rights, Bahrain Watch, and Privacy International. The complaint to the UK NCP was brought by Privacy International alone.

[184] See: Final statement by the German NCP (21 May 2014), available at: https://www.oecdwatch.org/wp-content/uploads/sites/8/dlm_uploads/2021/03/erklaerung-der-deutschen-nationalen-kontaktstelle-englisch.pdf

[185] See: UK NCP, 'Privacy International & Gamma International UK Ltd: Final Statement After Examination of Complaint' (December 2014) ('UK NCP Final Statement'), available at: https://www.oecdwatch.org/wp-content/uploads/sites/8/dlm_uploads/2021/03/UK%20NCP%20final%20statement%20Gamma.pdf

it had supplied spyware technology to Bahrain, and accordingly the NCP did not verify any direct link between the company and any adverse human rights impacts of digital surveillance in that country,[186] but did conclude that Gamma had failed to carry out appropriate due diligence, failed to have a policy commitment to respect human rights or encourage business partners to respect human rights, and failed to provide for, or co-operate with, remediation of human rights impacts.[187] As a result, the NCP concluded that Gamma's approach was '*not consistent with the general obligations to respect human rights*'[188] and that '*the company's overall engagement with the NCP process ha[d] been unsatisfactory, particularly in view of the serious nature of the issues raised.*'[189]

83. Despite that adverse finding, there is no evidence that Gamma has altered any of its processes so as to prevent or mitigate adverse human rights impacts in the future. The UK NCP requested an update in 2015 regarding any such progress, but Gamma did not respond,[190] prompting the NCP to observe that it '*can only conclude that [Gamma] has made no progress (or effort) towards meeting the recommendations made*' by the NCP,[191] and that '*Gamma's failure to engage is … an individual choice rather than an unavoidable result of the nature of its business. It is a choice that is likely to leave Gamma open to further complaints and challenges, as well as to negative assumptions from stakeholders.*'[192]

84. The third case in relation to the surveillance technology was brought by the NGO the Society for Threatened Peoples ('STP') against the Swiss bank UBS alleging that UBS has breached its due diligence obligations in relation to its investments in the Chinese technology company Hikvision, which has installed mass surveillance systems used in the monitoring of the Uyghur population in Xinjiang province, and in the operation of internment camps there. The NCP initially assessed that a link between UBS and human rights violations carried out in China could plausibly be argued by virtue of UBS investment,[193] and offered a mediation process by which actions on UBS's part to address the risk of such investment having adverse human rights impacts could be further

---

[186] UK NCP Final Statement, [51]-[59].

[187] UK NCP Final Statement, [61]-[68].

[188] UK NCP Final Statement, [69].

[189] UK NCP Final Statement, [70].

[190] UK NCP, 'Follow Up Statement After Recommendations in Complaint from Privacy International against Gamma International' (February 2016) ('UK NCP Follow Up Statement'), [5], available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/847364/uk-ncp-follow-up-statement-privacy-international-gamma-international.pdf

[191] UK NCP Follow Up Statement, [9].

[192] UK NCP Follow Up Statement, [11].

discussed. In its final statement in December 2021, the Swiss NCP noted that the mediation had reached an impasse, with UBS having made no undertakings to take responsibility for human rights impacts from its passive investment funds, or to restructure its financial products to enable it to exit investment scenarios found to be putting the fund in a position of failing to respect human rights.[194]

85. From the Special Rapporteur's assessment the experience of complaints through the OECD NCP framework alleging breaches by businesses involved in the use of surveillance technology of their corporate responsibility to respect human rights is thus not encouraging from the perspective of human rights compliance. The process has been marked by non-engagement by the businesses and outcomes which are both inconclusive and, in any event, unenforceable. That can be attributed to two key limitations of the process. First, the absence of any coercive power on the part of the NCP to require disclosure of information (in contrast, say, to the investigatory powers of law enforcement in criminal proceedings or the obligations of document discovery arising in civil litigation). And second, the absence of any threat that binding sanctions (whether in the form of mandatory orders about conduct or financial penalties) may be imposed by the NCP.

86. In the absence of a multilateral solution, then, domestic legal frameworks could theoretically offer an alternative for enforcing human rights standards for businesses engaged in the supply of surveillance technology. Regrettably, no State has implemented a comprehensive statutory framework imposing mandatory compliance by businesses with the Guiding Principles, but, as set out in their National Action Plans, certain States have adopted statutory provisions creating (often largely procedural)[195] obligations for businesses in relation to certain human rights subject matter.

87. Many jurisdictions enshrine in statute certain reporting requirements relating to businesses' activities which may have an impact on human rights. In the European Union, businesses above a certain size are required to include in their annual reports a

---

193 Switzerland NCP, 'Initial Assessment: Specific Instance Regarding UBS Group AG submitted by the Society for Threatened Peoples Switzerland' (20 January 2021), p6, available at: https://www.oecdwatch.org/wp-content/uploads/sites/8/dlm_uploads/2021/04/Swiss-NCP_-Initial-Assessment_UBS_STP.pdf

194 Switzerland NCP, 'Final Statement: Specific Instance Regarding UBS Group AG submitted by the Society for Threatened Peoples Switzerland' (20 December 2021), pp4-5, available at: https://www.oecdwatch.org/wp-content/uploads/sites/8/dlm_uploads/2022/02/SwissNCP_Final-Statement_UBS_STP_forPublication.pdf

195 For a critique of the utility of procedural obligations with respect to corporate respect for human rights, see: G Quijano and C Lopez, 'Rise of Mandatory Human Rights Due Diligence: A Beacon of Hope or a Double-Edged Sword?' (2021) 6(2) *Business and Human Rights Journal* 241.

“

It feels like the walls are closing in on me, that I cannot protect the children and that we are not safe anywhere. I feel like I am defending myself against a whole ‘state’. Even in our own home they will be towering over us.

”

- Princess Haya, UAE
Ex-wife of Sheikh Mohammed bin Rashid al-Maktoum

Souce: Dan Sabbagh, “ ‘The walls are closing in on me’: the hacking of Princess Haya”, *The Guardian* (6 October 2021), https://www.theguardian.com/world/2021/oct/06/walls-closing-in-story-behind-princess-haya-hacking-ordeal.

non-financial statement of, among other things, the impact of their work on the environment and on respect for human rights.[196]

88. A proposal announced in April 2021 by the European Commission for a European Union mandatory human rights due diligence directive,[197] while repeatedly delayed, was released in February 2022.[198] This proposal, which is welcome, would require EU States, inter alia, to adopt legislation requiring large numbers of companies (identified either by size or sector) to integrate due diligence regarding potential adverse human rights impacts of their business activities into their corporate policies,[199] to identify actual and potential such adverse human rights impacts,[200] to take steps to prevent or mitigate adverse impacts,[201] and to bring known adverse impacts to an end.[202] Under the proposal, Member States would also be obliged to establish supervisory authorities to monitor businesses' compliance with their obligations,[203] with powers to sanction infringements.[204] In addition, the proposal seeks that Member States create a system of civil liability for companies if they fail to prevent, mitigate, or bring to an end adverse human rights impacts arising from their business which ought to have been dealt with.[205]

89. The proposal has been forwarded to the European Parliament and the Council, and it can be expected that, given its scope and given the fact that only very few EU Member States have any experience with legal regulation of companies' human rights impacts, there will be substantial negotiation and delay prior to any serious consideration of adoption. Prior to any harmonizing instrument applying to corporate human rights obligations generally, the domestic legal landscape of corporate human rights obligations is a patchwork of rules relating to specific subject matter, bolstered in some systems by broad doctrines regarding duties of care drawn from the general law of tort or delict.

---

196 Directive 2014/95/EU of the European Parliament and of the Council of 22 October 2014 amending Directive 2013/34/EU as regards disclosure of non-financial and diversity information by certain large undertakings and groups, OJ L 330, 15 November 2014, pp1-9, Article 1 inserting Article 19a in Directive 2013/34/EU.

197 Following a European Parliament resolution passed with overwhelming support in favour of the proposal. See: European Parliament Resolution of 10 March 2021 with Recommendations to the Commission on Corporate Due Diligence and Corporate Accountability (2020/2129(INL)).

198 European Commission, Proposal for a Directive of the European Parliament and of the Council on Corporate Sustainability Due Diligence and amending Directive (EU) 2019/1937, COM(2022) 71 final ('Proposal for Due Diligence Directive').

199 Proposal for Due Diligence Directive, Article 5.

200 Proposal for Due Diligence Directive, Article 6.

201 Proposal for Due Diligence Directive, Article 7.

202 Proposal for Due Diligence Directive, Article 8.

203 Proposal for Due Diligence Directive, Article 17.

204 Proposal for Due Diligence Directive, Article 20.

205 Proposal for Due Diligence Directive, Article 22.

90. A number of jurisdictions (including the US state of California,[206] the United Kingdom,[207] and Australia)[208] have adopted laws which require businesses to make disclosures regarding the actions they have taken to ensure that slavery and human trafficking is not taking place in their own operations, or in those of enterprises in their supply chains. Some jurisdictions have gone further, requiring not just reporting and transparency, but *active steps* on the part of businesses to exercise reasonable due diligence enquiries and put in place mitigation strategies to minimize certain human rights impacts. In France, the so-called 'Duty of Vigilance Act'[209] introduced in 2017 requires large French enterprises to publish annual vigilance plans which detail the practical due diligence steps the enterprise intends to take to prevent adverse human rights impacts from their own activities, and from the activities of companies under their control, their suppliers and subcontractors, and those with whom they have an established commercial relationship.

91. Enterprises can be challenged on the adequacy of their vigilance plans, can be obliged to 'effectively implement' them, and can be subject to financial sanctions for breaches. Interim decisions in late 2021 confirmed that issues of compliance by enterprises are justiciable in the ordinary French courts,[210] and a number of cases are ongoing against large French enterprises in respect of the adequacy of their plans to mitigate environmental damage from their operations. In the Netherlands, the Child Labour Due Diligence Law, expected to come into force in 2022, similarly requires enterprises to identify and take active steps to mitigate risks of child labour emerging in their business operations or supply chains.[211] The United States Department of State has released the non-binding Surveillance Due Diligence Guidance to assist surveillance technology exporters with criteria to evaluate whether to proceed with a sale, urging businesses to '*use these resources when considering exports of technology that could be used by nefarious actors to commit human rights abuses.*'[212]

---

206 California Transparency in Supply Chains Act of 2010 (SB 657).

207 Modern Slavery Act 2015.

208 *Modern Slavery Act 2018 (Cth).*

209 Law No 2017-399 of 27 March 2017, 'Relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre. For an overview, see : S Cossart et al., 'The French Law on Duty of Care: A Historic Step Towards Making Globalization Work for All' (2017) 2(3) *Business and Human Rights Journal* 317; and E Savourey and S Brabant, 'The French Law on the Duty of Vigilance: Theoretical and Practical Challenges Since Its Adoption,' (2021) *6 Business and Human Rights Journal* 141.

210 See: *Notre Affaire à Tous et al. c. Total* (18 November 2021, Versailles Court of Appeal); and Les Amis de la Terre et al. c. Total (15 December 2021, Versailles Court of Appeal).

211 Wet Zorgplicht Kinderarbeid [Child Labour Due Diligence Law].

92. Such due diligence laws are welcome: they represent good practice which goes some way to responsibilizing private enterprise to play a part in the prevention of adverse human rights consequences arising from their products. But even to the extent that due diligence laws are in place, their practical impact may be questioned when the potential uses of spyware technology are, by their nature, covert and unpublicized. When questioned by the European Parliament's committee on Pegasus spyware in June 2022, the Chief Compliance Officer of NSO Group, Mr Chaim Gelfand insisted (without providing any details) that '*[e]very customer we sell to, we do due diligence on in advance in order to assess the rule of law in that country. But working on publicly available information is never going to be enough.*'[213] This statement is difficult to reconcile with the considerable body of evidence suggesting that States purchasing NSO Pegasus spyware were using it in clear violation of human rights.

93. Aside from this selection of specific reporting and due diligence laws, businesses also – like other persons – are typically capable of owing general duties of care under domestic doctrines in the law of tort or delict. The content of those general duties – generally speaking, to act with reasonable prudence to avoid foreseeable types of harm being caused to persons foreseeably capable of being affected by one's actions[214] – can theoretically overlap with substantive human rights protections, particularly with respect to human rights addressed to physical safety and security (such as the right to life,[215] the right to freedom from torture and cruel or inhuman treatment or punishment,[216] and the right to liberty and security of the person).[217]

94. In the Special Rapporteur's view reliance upon adventitious overlaps with existing general duty of care doctrines is not, however, a realistic means of guaranteeing respect by spyware manufacturers for human rights by alternative means. That is for at least four reasons.

---

212 See: OHCHR, 'The Practical Application of the Guiding Principles on Business and Human Rights to the activities of technology companies,' UN Doc. A/HRC/50/56 (21 April 2022), [17], and the US submission to the OHCHR Expert Consultation, available at: https://www.ohchr.org/sites/default/files/2022-03/UnitedStates.pdf

213 See: Remarks of Mr Chaim Gelfand to Committee of inquiry to investigate the use of Pegasus and equivalent surveillance spyware (21 June 2022). Video of hearing available at: https://multimedia.europarl.europa.eu/en/webstreaming/pega-committee-meeting_20220621-1500-COMMITTEE-PEGA

214 For general statements of analogous doctrines, see: in respect of the United States of America, Restatement (Third) of Torts: Liability for Physical Harm § 3 (PFD No 1, 2005) and Restatement (Second) of Torts § 282 (1965); in respect of English law and cognate common law systems, *Donoghue v Stevenson* [1932] AC 562 (HL); in respect of French law and cognate civil systems, Code Civil 1804, Articles 1382-1383 (and subsequent amendments and local versions).

215 ICCPR, Article 6(1).

216 ICCPR, Article 7.

217 ICCPR, Article 9.

95. First, the subject matter of general doctrines of duty of care is typically restricted to physical harm, and does not extend to more abstract (but nonetheless fundamental) values such as privacy, free expression, freedom of assembly, and freedom of religion.

96. Second, the extent to which business enterprises may be liable for actions carried out by subsidiaries (even if sanctioned/with the knowledge of parent companies) or carried out in other jurisdictions is a complex and contested issue.[218] Recent cases in the UK,[219] Canada,[220] New Zealand,[221] and the Netherlands[222] have accepted the position in principle that parent companies may be liable for subsidiaries' conduct in certain circumstances without formally directing that conduct.

97. As for the United States, in the early years of this century, human rights proponents often made use of the historic US Alien Tort Statute ('ATS'), a law which provides that the federal courts of the United States have jurisdiction in respect of civil claims brought by '*aliens*' (i.e. foreign nationals located within the US) for '*torts committed in violation of the law of nations or a treaty of the United States.*'[223] The law provides a basis for claims involving violations of well-defined and universally-accepted norms of international law. The statute has been used to sue foreign government officials for acts of torture,[224] and was prayed in aid by human rights activists alleging that corporations have either directly violated international law, or aided and abetted violations committed by others. The scope for ATS claims as a means of individual redress was drastically reduced, however, by the decision of the Supreme Court in *Kiobel v Royal Dutch Petoleum Co*.[225]

98. The majority of the Supreme Court in *Kiobel* retained the possibility of ATS claims which do '*touch and concern*' the territory of the United States, provided that those claims '*do so with sufficient force to displace the presumption against extraterritorial application.*'[226] But the Supreme Court has subsequently clarified and arguably tightened the criteria

---

218 See, for example, the tentative suggestion of potential parent company liability for subsidiaries' conduct in

219 *Okpabi and ors v Royal Dutch Shell plc and anor* [2021] 1 WLR 1294 (UKSC); and *Lungowe v Vedanta Resources plc* [2020] AC 1045 (UKSC).

220 *Nevsun Resources Ltd v Araya and ors*, 2020 SCC 5.

221 *James Hardie Industries plc v White* [2018] NZCA 580; and *James Hardie Industries v White* [2019] NZSC 39.

222 *Milieudefensie and ors v Shell Petroleum NV and ors* [C/09/365498/HA ZA 10-1677] and [C/09/330891/HA ZA 09-0579]; [C/09/337058/HA ZA 09-1581] and [C/09/365482/HA ZA 10-1665].

223 28 USC §1350 (also known as the Alien Tort Claims Act 1789).

224 Such as the successful US$22 million damages claim brought by victims of torture in Liberia against Charles McArthur Emmanuel, the son of President Charles Taylor and the commander of the Liberian government's Anti-Terrorism Unit during the Liberian Civil War: *Kpadeh v Emmanuel* 261 FRD 687 (S.D. Fla. 2009).

225 *Kiobel v Royal Dutch Petroleum Co* 569 US (US Supt Ct 2013).

226 Ibid., p14.

applying to such claims, holding in the case of *Nestlé USA v Doe* that the claimants could not establish that their claim displayed a sufficient link to USA activities.[227] The Supreme Court held that the mere fact of general corporate activity in the United States, even if it practically facilitated violations of international law abroad, was insufficient to allow recourse to the US courts under the ATS. Claimants would need, therefore, to demonstrate that key decisions and acts of assistance for the alleged international violations actually took place within the United States.[228]

99. In the Special Rapporteur's view the absence of a clear worldwide consensus on enterprises' liability for overseas and/or subsidiary or agent conduct undermines any deterrent force against harmful corporate behaviour that tort or delict liability could potentially present. To the contrary, it simply invites enterprises to engage in jurisdictional arbitrage and procedural skirmishes to avoid liability on technical grounds.

100. Third, the interrelationship between corporate actions and State authority in the use of spyware internationally creates great complexity and substantial room for contestation as to the possibility of individual claimants seeking redress against allegedly unlawful State-controlled surveillance. As a general principle of international law which is often implemented via national legislation, domestic courts (as opposed to international for a like the International Court of Justice) typically decline jurisdiction to rule upon cases which raise allegations as to the conduct of foreign States and their official agents. This doctrine of foreign state immunity holds that official foreign State organs cannot be sued in domestic courts without their consent,[229] except in certain narrowly-defined circumstances. Allegations of causing physical injury is typically one such exception (which provided the route to potential liability of the KSA in the *Al-Masarir v Kingdom of Saudi Arabia* case in August 2022 in the UK),[230] but that exception will only apply in cases of surveillance being linked to death or

---

227 *Nestlé USA, Inc. v Doe et al.* 593 US_ (2021).

228 As was the case in *Al Shimari v CACI Premier Technology Inc* No. 13-1937 (4th Circuit 2014).

229 See, for instance: H Fox and P Webb, *The Law of State Immunity* (3rd ed, 2015). See the attempted codification of the doctrine of foreign state immunity in: UN General Assembly, Resolution 59/38 United Nations Convention on Jurisdictional Immunities of States and Their Property, UN Doc. A/RES/59/38 (2 December 2004) (not yet in force).

230 *Al-Masarir v Kingdom of Saudi Arabia* [2022] EWHC 2199 (QB), [191] (Knowles J).

231 Such a change has been urged by the Special Rapporteur on freedom of opinion and expression: A/HRC/41/35, [55].

physical mistreatment, and so will not be effective to facilitate claims based on non-physical interferences with privacy, expression, political participation, etc. Without a fundamental change to well-established jurisprudence,[231] then, the principle of sovereign immunity represents a considerable obstacle to recourse through domestic courts.

101. Fourth, the nature of spyware use being covert means that targets typically are either unaware of, or only have partial evidence of, the fact of their having been targeted at all. While cases may be established on the balance of probabilities on the basis of leaked information or forensic digital analysis which identifies tell-tale signs of spyware use, the absence of a comprehensive, dependable, and complete record of spyware operations renders it difficult for victims to establish the full facts of their claim, and difficult for judicial authorities to conduct adequate investigations of all the circumstances.

102. The sample size of domestic litigation brought by those affected by spyware infiltration (both human victims and technology companies whose systems have been unlawfully breached)[232] is small. But a marked feature of such cases has been the argument raised by the spyware corporations that any acts they have carried out were committed in the corporations' capacity as agents of foreign State customers, such that the doctrine of foreign state immunity should prevent the court considering the claim. NSO relied on this argument in response to the claim brought in US Federal Court by WhatsApp Inc for alleged wrongful interference with its network and subscribers, claiming that, as the company only deals with and provides capacity to foreign State agencies, it should be treated by analogy with official agents of foreign States. The Circuit Court of Appeals rejected the argument in November 2021, holding that the wording of the United States Foreign Sovereign Immunity Act meant that only

---

231 Such a change has been urged by the Special Rapporteur on freedom of opinion and expression: A/HRC/41/35, [55].

232 Private ICT companies have threatened litigation against spyware companies on a handful of occasions, claiming that intrusive software harms their own operations and users, and violates their intellectual property by mimicking their own products. See: the 2013 'cease and desist' letter from Mozilla to Gamma Group One set out in A Fowler, 'Protecting our brand from a global spyware providers,' The Mozilla Blog (13 April 2013), available at: https://citizenlab.ca/wp-content/uploads/2017/03/citizenlab_whos-watching-little-brother.pdf. See also the action brought by Meta companies WhatsApp and Facebook against NSO in 2019, a summary of which is set out in M Dvilyanski, D Agranovich, and N Gleicher, 'Threat Report on the Surveillance-for-Hire Industry,' Meta (December 2021), available at: https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf The low incidence of such litigation brought by private companies against spyware technology which affects commercial interests is perhaps surprising, given that the legal framework protecting intellectual property rights is well-established. See: S McKune and R Deibert, 'Who's Watching Little Brother?: A Checklist for Accountability in the Industry Behind Government Hacking,' Univesity of Toronto: Munk School of Global Affairs (2 March 2017), pp20-21.

“This operation wrecked the work of staff and destabilized my campaign... I don’t know how many votes it took from me and the entire coalition.”

- Krzysztof Brejza
Opposition politician, Poland

Source: Vanessa Gera and Frank Bajak, “Polish opposition senator hacked with spyware”, *AP* (23 December 2021), https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab.

official *foreign State* entities and not *corporate entities* were entitled to that protection.[233] NSO has, however, petitioned the Supreme Court for a review of the Circuit Court of Appeals decision.[234] The Special Rapporteur urges the US Supreme Court to take a robust view of NSO's claimed entitlement to State immunity as a defence to facilitating wrongful interference with human rights.

103. Different jurisdictions have slightly divergent wordings for their foreign state immunity statutes. Interpretations of how common law and civil law doctrines ought to apply to the novel situation of corporate entities being closely tied with State security agencies may well vary from country to country. As a result, the complications over how immunity doctrines may apply to the position of spyware corporations acting in concert with State agencies will likely require clarification through a lengthy process of multiple judicial determinations. For instance, in the claims brought in the English High Court by Mr Anas Altikiri, Mr Mohamed Kozbar, and Mr Yahya Assiria against the UAE, KSA, and NSO Group in relation to alleged Pegasus targeting, NSO has claimed at the pre-action stage that, insofar as any responsibility attaches to the company, it can only be by virtue of its link to State agencies, and that foreign state immunity should bar the claim.[235]

104. As the former UN Special Rapporteur on the promotion and protection of freedom of opinion and expression has noted, in theory each of the various barriers to domestic litigation being an effective mechanism for bringing accountability to purveyors of spyware technology for harms arising from the end use of that technology could be the subject of specific legislative measures to facilitate lawsuits and remedies for victims.[236] To be effective, however, such reforms would need to be comprehensive – addressing a wide

---

[233] *WhatsApp Inc. and Facebook Inc. v NSO Group Technologies and Q Cyber Technologies* No. 20-16408 (9th Circuit Court of Appeals 2021).

[234] See: https://www.supremecourt.gov/DocketPDF/21/21-1338/220429/20220406140142533_2022-04-06%20NSO%20Cert%20Petition%20FINAL.pdf. The decision of the Supreme Court remains awaited.

[235] See: B Goodwin, 'NSO Group faces court action after Pegasus spyware used against targets in UK,' *ComputerWeekly* (20 April 2022), available at: https://www.computerweekly.com/news/252516106/NSO-Group-faces-court-action-after-Pegasus-spyware-used-against-targets-in-UK

[236] See: Kaye, above n 104, 490. A/HRC/41/35, [55].

variety of doctrines of standing, justiciability, sovereign immunity etc - and internationally-coordinated, lest new legal tests simply provide opportunities for arbitrage and differentiation between different legal fora. **The Special Rapporteur stresses that any system for regulation and legal accountability for the use of spyware would - it is important to note - also require that the spyware tools be redesigned so as to ensure that there remains in each instance a permanent and indelible record of the deployment of the technology, such that, if judicial consideration comes to be required, there is an adequate evidential record which could support accurate findings upon lawfulness or breach.**

Regulation of States Allowing Trade in Surveillance Technology

105. The alternative to direct regulation of the business enterprises responsible for the manufacture and sale of surveillance technology (through laws requiring human rights compliance or through general laws covering similar subject matter) is regulation of the trade in surveillance technology by imposing supply-side restrictions when States are considering authorizing such exports across borders.

106. **Export control restrictions upon trade by spyware companies must be distinguished from sanctions on trade *to* spyware companies.** Following the Pegasus revelations, the United States, for instance, retaliated directly against a number of spyware companies with sanctions, adding NSO, Candiru, a Russian company known as Positive Technologies, and a Singaporean company known as Computer Security Initiative Consultancy PTE to the US trade blacklist.[237] That meant that US companies could no longer provide goods or services (such as intelligence about computer system vulnerabilities)[238] to the blacklisted entities. In the Special Rapporteur's view such barriers are of limited impact in slowing the development of spyware technology, since relevant goods and technical expertise can readily be sourced elsewhere, and blacklists do not prevent the spyware manufacturers from selling spyware,[239] or even part ownership of the manufacturer itself, into the sanctioning country.[240]

107. As for export controls, the key overarching framework is the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies ('the Wassenaar Arrangement'). The Wassenaar Arrangement is a multilateral export control regime founded in 1996 which currently has 42 participating States, including a substantial number of States home to companies responsible

---

237 See: C Bing, 'US blacklists Israeli hacking tool vendor NSO Group,' *Reuters* (3 November 2021), available at: https://www.reuters.com/article/usa-cyber-nso-group-idCAKBN2HO1L0; and D Sanger, N Perlroth, A Swanson, and R Bergman, 'US Blacklists Israeli Firm NSO Group Over Spyware,' *The New York Times* (3 November 2021), available at: https://www.nytimes.com/2021/11/03/business/nso-group-spyware-blacklist.html

238 It has been reported that NSO offered representatives of the American mobile phone security firm Mobileum 'bags of cash' for access to an exploitable global mobile phone network. See: S Kirchgaessner, 'NSO offered US mobile security firm "bags of cash," whistleblower claims,' *The Guardian* (1 February 2022), available at: https://www.theguardian.com/news/2022/feb/01/nso-offered-us-mobile-security-firm-bags-of-cash-whistleblower-claims.

239 As NSO's creditors such as Credit Suisse reportedly encouraged. See: K Wiggins, O Aliaj, and M Srivastava, 'Credit Suisse pushed for spyware sales at NSO despite US blacklisting,' *Financial Times* (7 June 2022), available at: https://www.ft.com/content/e55a92d4-6a0a-4284-aa22-639dad5f2b65

240 See: K Anzalone and W Porter, 'Israeli Spyware Firm Seeking to Sell Hacking Tech to US Defense Contractor,' *The Libertarian Institute* (15 June 2022), available at: https://libertarianinstitute.org/news-roundup/israeli-spyware-firm-seeking-to-sell-hacking-tech-to-us-defense-contractor/; and E Nakashima and C Timberg, 'White House has security concerns about any deal for NSO hacking tools,' *The Washington Post* (14 June 2022), available at: https://www.washingtonpost.com/national-security/2022/06/14/l3harris-nso-sale-pegasus/ Further, there are reports of attempts to lobby the Biden Administration to reverse the blacklisting. See: B Ravid, 'Scoop: Israelis push US to remove NSO from blacklist,' *Axios* (8 June 2002), available at: https://www.axios.com/2022/06/08/nso-pegasus-israel-us-commerce-blacklist

for the manufacture and export of surveillance technology, including the United States of America, the United Kingdom, France, Germany, Russia, and Italy.[241] But a number of States with significant industries in the field of arms and in particular dual-use cyber technology, namely China, Israel, and Singapore, are in the Special Rapporteur's view regrettably not members (albeit that domestic legislation in each country establishes export control arrangements which identify some of the Wassenaar Agreement list of goods).[242]

108. The basic structure of the Wassenaar Arrangement is a regularly-updated list of conventional arms and dual-use goods and technologies ('dual-use' goods or technologies being those not exclusively designed for, but capable of, military applications), agreed by the member States by consensus. The objective is that States should seek to restrict the export of these goods and technologies to other States in circumstances where they may be misused by State or non-State entities. Each State undertakes to operate an export control regime in respect of the listed goods and technologies, and to transparent sharing of information on export approvals and denials so that international arms trade trends and risks can be better identified.

109. The Wassenaar Arrangement does not itself involve a legally-binding multilateral treaty. Member States do not automatically impose export restrictions on goods merely because of their inclusion on the Wassenaar list, but most Member States (whether through regional action at the European Union level or individually) in practice update their domestic export control regimes regularly to give effect to a relatively consistent approach worldwide among members.

110. In 2012 and 2013, amendments were introduced to add certain types of cyber and digital surveillance

---

241 See, generally: https://www.wassenaar.org

242 UN Working Group on Business and Human Rights, 'Responsible business conduct in the arms sector: Ensuring business practice in line with the UN Guiding Principles on Business and Human Rights,' available at: https://www.ohchr.org/sites/default/files/2022-08/BHR-Arms-sector-info-note.pdf

technologies including IMSI catchers, certain applications related to intrusion software, and IP network surveillance systems.[243] The inclusion of intrusion software-related applications was controversial, with arguments from the industry that it could apply inappropriately to cyber security applications (such as updating antivirus programs and forensic examination applications used for security testing).[244] These were dealt with by way of specific exemptions to carve out legitimate intrusion tools. As the IP network surveillance systems, the specified scope of the controlled technologies is very narrow, being restricted to surveillance targeting traditional Internet communications via web and email, and even then only on a 'carrier class IP network' (that is, a national Internet system).[245] Notably, surveillance tools designed for many kinds of metadata analysis, or for different types of networks (local area networks or non-standard communication systems) fall outside the definition completely, as a range of technical experts have observed.[246]

111. The national attempts to implement the Wassenaar Arrangement system of controls on the trade of surveillance technology vividly dramatize the challenges for effective protection of human rights of potential targets in the field of digital surveillance. In the United States of America, the implementation of controls to give effect to the Wassenaar Arrangement undertakings is governed by a complex statutory framework with various licensing and enforcement bodies empowered by the Export Control Reform Act 2018 ('ECRA')[247] and the Export Administration Regulations,[248] for which the Department of Commerce is largely responsible. The system applies to 'export, re-export, or in-country transfer' in relation to US jurisdiction, and can apply to non-US companies and even non-US-made products if they contain US-made technological elements. While formally seeking to regulate many of the technologies on the Wassenaar Arrangement list, the US regime, and particularly the ECRA enacted in 2018, grants

---

243 See: Controlled Categories 4.A.5, 4.D.4, 4.E.1.c, 5.A.1.f, and 5.A.1.j.

244 F Bohnenberger, 'The Proliferation of Cyber-Surveillance Technologies: Challenges and Prospects for Strengthened Export Controls' (2017) 3 *Strategic Trade Review* 81, 86-87.

245 H Kim, 'Global Export Controls of Cyber Surveillance Technology and the Disrupted Triangular Dialogue,' (2021) 70(2) *International & Comparative Law Quarterly* 379, 393.

246 Bohnenberger, above n 244; and T Maurer, E Omanovic, and B Wagner, 'Uncontrolled Global Surveillance: Updating Export Controls to the Digital Age' (New America Foundation, Digitale Gestellschaft, and Privacy International, March 2014), p31.

247 The ECRA formed part of the 'John S McCain National Defense Authorization Act for Fiscal Year 2019,' 132 STAT. 1636 (§§ 1741-1793).

248 15 C.F.R. § 730 et seq.

a very wide discretion to executive arm of government to determine the permissible circumstances of the trade, both according to technologies for export and recipient entities.

112. The key criterion for determining licenses for technology export is what is deemed by the Department of Commerce to be 'essential to national security,'[249] and the US government retains the option unilaterally to define controlled technologies without any consistency with multilateral agreement. Under the ECRA, certain exports of surveillance technology products have been prevented (including any to the Chinese firm Huawei Technologies or its non-US affiliates), but on the basis of *national security and foreign policy* concerns rather than potential human rights risks to persons unlawfully targeted by Chinese government surveillance.[250] In the Special Rapporteur's view if governmental decision-makers are not directed actively to consider, in terms, potential human rights impacts of exports, it should come as no surprise if such potential human rights impacts, particularly those which may be of a more abstract type than physical risks, are not adequately guarded against.

113. In the European Union, the devolved export control mechanism which gives effect to the overarching obligations undertaken under Wassenaar Arrangement with respect to 'dual-use' technologies is the Recast Dual-Use Regulation, recently updated in September 2021.[251] The Recast Dual-Use Regulation sets out a list of specified dual-use technologies, including surveillance technologies[252] identified under the Wassenaar Arrangement, and provides for the free transfer of dual-use items within the EU, but imposes restrictions on the transfer and trade outside the EU. Member States are entitled to augment the list '*for reasons of public security or human rights considerations.*'[253] In respect of such technologies, Member States are obliged to take into account a range of considerations including

---

249 ECRA, § 1758(a).

250 See: Bureau of Industry and Security, 'Addition of Entities to the Entity List, Federal Register,' BIS Rule, 84 F.R. 22961 (16 May 2019); and Bureau of Industry and Security, 'Addition of Entities to the Entity List and Revision of Entries on the Entity List,' BIS Rule, 84 F.R. 43493 (19 August 2019).

251 See: Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 Setting Up a Union Regime for the Control of Exports, Brokering, Technical Assistance, Transit and Transfer of Dual-Use Items (Recast) ('Recast Dual-Use Regulation') replacing the Council Regulation (EC) No 428/2009 of 5 May 2009 Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-Use Items. Export control of conventional military technology is governed by the separate European Council Common Position which cross-refers to the Common Military List. See: Council Common Position 2008/944/CFSP of 8 December 2008 Defining Common Rules Governing Control of Exports of Military Technology and Equipment, OJ L 335, 13 December 2008 ('EU Common Position'), pp99-103; and Common Military List of the European Union adopted by the Council on 17 February 2020, OJ C 85, 13 March 2020, pp1-37.

252 Recast Dual-Use Regulation, Annex I.

253 Recast Dual-Use Regulation, Article 9(1).

'*the obligations and commitments they have each accepted as members … by ratification of relevant international treaties*'[254] and '*considerations about intended end-use and the risk of diversion.*'[255]

114. These provisions provide the legal framework for Member State authorities to take into account the potential adverse effect of any technology exports on the protection of human rights (and thus on the Member State's own obligations under multilateral human rights treaties not to facilitate human rights breaches whether domestic or extraterritorially). In this respect, the recitals to the Regulation specifically note that '*[w]ith regard to cyber-surveillance items, the competent authorities of the Member States should consider in particular the risk of them being used in connection with internal repression or the commission of serious violations of human rights and international humanitarian law.*'[256]

115. The limiting criterion upon exports of surveillance technology is not therefore a hard-edged one (whether or not the technology appears on a relevant list). The limiting criterion is instead whether or not the relevant national authority has *properly* (within the bounds of its own national law) taken into account its international treaty obligations, including its human rights obligations. In the Special Rapporteur's view that is a restriction of limited practical effect. And the recent litigation in the United Kingdom challenging the export of conventional arms to the Kingdom of Saudi Arabia for use in the military conflict in Yemen provides a stark example of just how limited.

116. That litigation related to the continued export of conventional arms, rather than dual-use technology, under UK rules[257] which (prior to Brexit) sought to give effect to the precursor of the EU export control regime and illustrates the issues well.[258] The structure of the restrictions was that the government was required to give proper consideration to the conduct of recipient countries and refuse exports where there was a *clear risk* that the items might be used for internal repression or might be used in the commission of a serious violation of international humanitarian law. That is very similar

---

254 Recast Dual-Use Regulation, Article 15(1)(a).

255 Recast Dual-Use Regulation, Article 15(1)(d).

256 Recast Dual-Use Regulation, Recital (2).

257 Export Control Act 2002, the Export Control Order 2008, and the UK 'Consolidated EU and National Arms Export Licensing Criteria.'

258 I.e. the EU Common Position, above n 251.

to the structure of the Recast Dual-Use Regulation in that it is focused on the adequacy of the exporting State's assessment of the potential end uses of the relevant goods.

117. At issue was the fact that, despite there being ample and undisputed evidence of the Saudi-led coalition in Yemen committing repeated violations of international law, the relevant UK government decision-maker nonetheless had concluded that there was no clear risk of any such violations in the future. In the first iteration of the litigation, the English Court of Appeal concluded that the UK government had acted unlawfully by failing even to consider the relevance of a historic pattern of violations.[259] But, tellingly, once the first case was concluded, the government simply 'remade' the decision, taking into account the historic record but deeming them 'isolated incidents' which did not indicate a future risk. That decision is currently under challenge.[260] But whatever the result in the renewed litigation, the scope for discretionary governmental decisions under an export control regime which only requires that decision-makers *take into account* human rights or international law impacts is clear. That is, governments may simply say that, having taken into account human rights records or potential risks, they are satisfied that the trade should go ahead. In the Special Rapporteur's view unless there is a bright-line rule which fixes governments with responsibility for human rights breaches, or requires exports to cease if there have been breaches or sufficiently serious concerns, the protection may well be illusory.

118. Export control systems rely on individual nations giving domestic effect to obligations in different terms relating to an inconsistent list of technologies. Further, those domestic obligations depend upon discretionary exercises *taking into account* (but not requiring strict observance with) human rights. These systems thus inevitably lead to inconsistencies, inviting jurisdictional arbitrage from would-be exporters or importers of surveillance technology for repressive uses identifying the countries with the weakest protections. Such systems, where remedies are through the indirect means of challenges to discretionary government approvals,

---

259 *The Queen (on the application of Campaign Against Arms Trade) v Secretary of State for International Trade* [2019] 1 WLR 5765 (CA).

260 D Sabbagh, 'High Court to Hear Legal Battle Over UK Arms Sales to Saudi Arabia,' *The Guardian* (22 April 2021), available at: https://www.theguardian.com/world/2021/apr/22/campaigners-to-challenge-decision-to-resume-selling-arms-to-saudi-in-high-court

also make for unpredictable legal outcomes which may have only tangential (and even then only temporary) impacts on the trade in the technologies posing risks to human rights in end use contexts.

119. Further, and even setting aside differences in approach between States, the whole architecture of export restrictions is premised on the assessment by exporting States ahead of time of the potential for misuse and harm contained in the products being exported. That requires sufficient transparency about those products' capabilities, and knowledge of their real-world applications and impacts. But the highly secret circumstances in which spyware is deployed (often without official acknowledgment, attribution, or record-keeping), and the opacity of spyware companies' operations, can mean that neither victims nor even State regulatory bodies are well apprised as to the existence of potential adverse human rights impacts, or the full scope of such potential harms.

120. **In the Special Rapporteur's view the upshot is that export control regimes are by themselves insufficient to regulate the commercial spyware industry in a manner capable of protecting international human rights.** Greater compliance with multi-lateral export control systems such as the Wassenaar Arrangement or substantively equivalent export control standards guarding against exports where risks of misuse exist has been recommended as a step towards greater regulation of the spyware industry,[261] and while greater participation would be welcome it is unlikely to deliver a robust solution to the dangers of misuse of surveillance technology. Whether through lack of searching inquiry, absence of available information at the time of licensing decisions being made, or lack of desire to curb growing spyware technology exports, the export control system has not prevented the rapid expansion of the burgeoning industry, its covert transfer internationally, or even eye-

[261] See the recommendation of the Special Rapporteur on freedom of opinion and expression at A/HRC/41/35, [57]-[59] and [66].

catching officially-acknowledged deals such as the export from Italy of Hacking Team's spyware to Kazakhstan or the export from Israel of NSO technology to the United Arab Emirates.[262] Export control mechanisms have not prevented, and appear incapable of preventing, ongoing human rights risks arising from the spyware trade.

121. A small number of States have recently promoted the establishment of a voluntary, non-binding code of conduct aimed at preventing the proliferation of software and other technologies used to enable serious human rights abuses, using the title the 'Export Controls and Human Rights Initiative.'[263] The details of that initiative remain to be seen, but given that the proposed initiative contemplates operating within the existing export controls system, in the Special Rapporteur's view the concerns raised above remain.

---

262 McKune and Deibert, above n 232, p7.

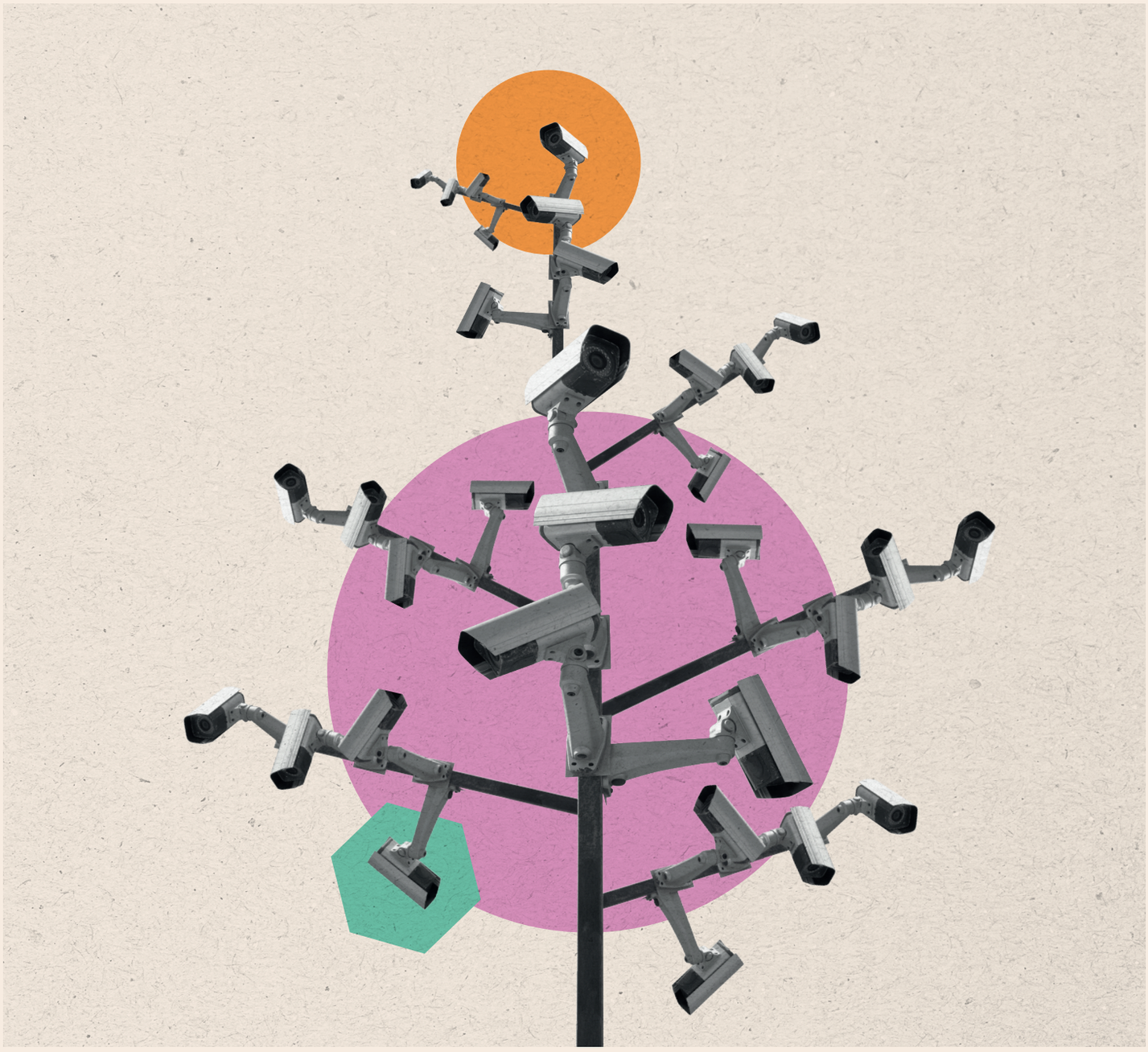
263 The governments of Australia, Canada, Denmark, France, the Netherlands, Norway, the United Kingdom, and the United States have expressed support for the Initiative. See: 'Joint Statement on the Export Controls and Human Rights Initiative,' available at: https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/10/joint-statement-on-the-export-controls-and-human-rights-initiative/

“If they have your phone, they have everything...”

- Hicham Mansouri
Investigative journalist, Morrocco

Source: https://forbiddenstories.org/journaliste/hicham-mansouri/

05 Part III: The Way Forward to More Effective International Regulation of Surveillance Technology



122. The Special Rapporteur concludes that the current response to the challenge posed to human rights by the extremely powerful tools of the contemporary spyware industry is fractured and inadequate. Direct approaches to the voluntary responsibility of corporations developing and selling the technology rely upon the UN Guiding Principles, which are affected by the absence of a binding enforcement arm, with the most sophisticated oversight regime (the OECD NCP system) rendered toothless through its inability to compel evidence or oblige engagement. An agreed international framework to render corporations' responsibilities in respect of actual and potential adverse human rights impacts is, despite some progress on a binding treaty, not realistic in the short term, given its very broad and ambitious scope.

123. Meanwhile, domestic law doctrines of tort/delict form an inconsistent patchwork, with ample room for argument about degrees of responsibility along transnational production chains, how human rights harms equate to (or diverge from) traditional models of physical harm, and how relationships between private entities and foreign sovereign entities ought to be dealt with. That confusing framework means that there is no obvious mechanism for accountability if corporations fail to advert to the harms to which their spyware technology may cause or contribute, and no clear deterrent to prevent producers from developing and trading in such technology without concern for its potential impacts.

124. At the same time, the typical system for controlling the export of products which risk human rights harms was developed for the radically different context of conventional arms. That export control system is predicated upon the assumption that the capacities and operations of products for export can transparently be assessed and well understood by public officials in advance. It also assumes that the nature of the products and their usage allows for a degree of visibility in the subsequent monitoring of how recipient countries put the products to use. In addition, the export control system grants exporting States generous latitude in their decision-making, providing the conditions for confusion, inconsistency, and arbitrage between jurisdictions. Gaps in the relevant information available to State decision-makers considering export authorizations, especially when coupled with discretionary decisions made against broad standards, render it unlikely that the existing export control system is capable of producing and enforcing consistent and meaningful international rules for the spyware trade.

[264] As first suggested by the Special Rapporteur on the freedom of opinion and expression at A/HRC/41/35, [60].

125. As a result, the way forward for regulation of the spyware trade requires a novel approach which avoids the gaps in the existing patchwork of purported oversight and accountability methods.

126. By suggesting a mechanism for an international legal response to the concerns raised by spyware technology, this paper should not be taken to convey a tacit endorsement that all forms of spyware technology are capable of lawful use, so long as a regulatory framework is agreed by States. Far from it. On the contrary, as set out above, a human rights analysis of the use of spyware in the counter-terrorism context suggests that spyware technology must at a minimum: (a) allow for users to specifically target certain data and metadata, rather than automatically monitor and record all data and metadata; (b) avoid automatically accessing data relating to contacts of targeted individuals, unless users specifically require that additional information for investigative purposes; (c) engineer mechanisms to prevent harmful use, such as flagging systems and 'kill switches' in cases of apparent misuse;[264] and, in any event, (d) create an indelible, permanent, and uneditable auditable record of what actions have been taken by the user of the spyware, including any interferences/modifications of data/metadata, when those occurred, and by whom they were effected so that the use of the tool can be verified, and its human rights compliance assessed after the fact by judicial authorities. Part of that indelible and uneditable record must be some

form of identifier or watermark such that judicial authorities overseeing complaints may verify the producer of spyware alleged to have been used against a victim and the customer to which that spyware was originally supplied and, from such source, can compel disclosure of the auditable record such that the legality of any use complained of can be adequately reviewed.

127. **Spyware which fails to display such features cannot, however otherwise tightly regulated, be capable of human rights compliance.** That is because such technology would be incapable of being deployed subject to the rules of necessity and proportionality, would be incapable of guaranteeing that evidence and/or privileged communications were not subject to monitoring or amendment, and would in any event fail to ensure that there was evidence of the nature and extent of the use of the tool which could be effectively reviewed and challenged by oversight and judicial bodies, and remedies provided for any breaches if necessary.

128. The recommendation for a regulatory framework to mitigate human rights violations arising from the development and trade of spyware technology, then, applies only insofar as spyware developers are capable of demonstrating – as part of their obligation to demonstrate due diligence – **that the technologies they provide to the market are subject to design limitations which render those products capable of human rights compliance at all.** Where products fail to conform with those basic limitations of capacity, and those basic record-keeping functions which allow for adequate oversight, no regulatory system will be able to remedy those fundamental legal defects.

129. As set out at the outset of this paper, the proposal of this regulatory framework should neither be considered an endorsement of the trade in, or use of, spyware, nor a non-endorsement of the calls by various civil society voices and human rights experts for an outright ban on the use of spyware. While the Special Rapporteur notes the force of those calls, the reality is that while such measures are debated and considered, the use of, and trade in, spyware technology continues, and the existing patchwork of controls discussed in this paper fail adequately to prevent the widespread violations of human rights which result.

130. Accordingly, and subject to those provisos, it is suggested that the necessary features of a regulatory framework, directly informed by the concerns identified in this paper, are:

130.1. That any framework be international in nature so as to avoid incentivizing jurisdictional arbitrage whereby entities developing and/or trading in spyware are capable simply of distributing their operations in different territories to avoid more onerous regulatory environments;

130.2. That any framework should depend upon State obligations as a means of regulating corporate behaviour so as to avoid corporate non-cooperation in the face of largely toothless private sector oversight infrastructure, such as the OECD NCP system to which surveillance companies have shown no serious respect;

130.3. That the obligations imposed on States be limited and strictly targeted to the spyware field so as to ensure that the international community is more likely to be capable of agreement. This minimizes the risk of the international community being unable (or unable without undue delay) to agree on aspects of a regulatory regime due to confusion or inconsistency in the understanding and application of relevant human rights standards (as is a risk for the Third Revised Treaty on business and human rights);

130.4. That the obligations relate to compulsory and concrete action on the part of States, rather than, for instance, the soft-edged and discretionary status quo of simply obliging State entities to take into account potential human rights impacts when approving export licences;

130.5. That the actions States are obliged to take in turn impose actual liabilities upon private entities responsible for the development and distribution of spyware technology. The confusion arising from attempts to regulate and incentivise companies' behaviour by exposing them to potential civil liability in tort/delict has led to dispute, argument, and opportunism. A model could see State agencies undertaking to impose direct and stand-alone liability upon spyware companies, actionable in civil suit, if, for instance, the

companies' spyware product can be shown to a Court's satisfaction to have infected a target and to have caused harm, and the company is unable to demonstrate, for instance, that they had undertaken thorough due diligence upon the potential end use and could satisfy the Court that there was no real risk of the technology being used to breach human rights;

130.6. A direct form of accountability, vindicable in domestic Court, would provide a range of benefits over non-judicial oversight mechanisms. For one thing, casting the relevant obligation as a new legal requirement within the existing structure of civil law allows for the use of ancillary legal tools to give effect to the accountability framework through, for instance, injunctive and interim relief, and forcing discovery/ disclosure of documents. Further, co-opting existing legal infrastructure provides a straightforward means by which Court judgments and orders made in one jurisdiction can be enforced against corporate assets held in other jurisdictions, giving teeth to any remedies obtained. These features set a legal accountability framework apart from a non-legal model, and argue in favour of the former. Of course, reliance upon domestic legal systems entails an element of variability, but that is an inevitable feature of judicial remedies (since even international rights courts first require the exhaustion of domestic remedies);

130.7. Further, if the structure of the liability imposed by States upon private entities were, as suggested, effectively to reverse the burden of proof, and require the private entity to demonstrate its due diligence efforts, this would avoid the particular problem encountered in the spyware field, whereby the opacity of the operations typically means that victims have very limited access to the evidence relevant to prove their own cases; and

130.8. The intention of the threatened imposition of this civil liability would be to cause developers of spyware tools either to obtain binding guarantees from State customers as to future use and human rights compliance, or to suspend supplies if inadequate guarantees are provided. This in turn is intended to stimulate

the State customers seeking access to spyware to put in place protections so that they are either in a position credibly to provide guarantees as to human rights compliance, or to sacrifice access to such technology. **The net result, it is intended, is that the trade in spyware technology is limited to contexts in which buyers and sellers share a proper, enforceable, commitment to minimizing adverse human rights impacts.**

131. This paper proposes a framework where countries agree that, for surveillance manufacturers to be able to operate and sell from their jurisdictions, they must agree in turn to direct legal liability for their (or their associated companies') export/trade of surveillance technology unless they can demonstrate that, by exercising due diligence and obtaining guarantees, they have established that there is no real risk that the end use of their spyware will breach human rights protections. A draft set of proposed binding inter-State commitments is set out below.

132. Different States may, depending upon their own constitutional arrangements, have different requirements to give effect within their national law to their undertakings at the international level. This paper does not seek to be prescriptive as to the logistics of State implementation of their undertakings, but does suggest that States should commit explicitly to ensuring that their undertakings are given domestic effect within a reasonable transition period (being two years, which is the typical implementation period required for the domestication of a European Union directive in national law).

133. The Special Rapporteur considers that the adoption of a proposed international regulatory system such as the method outlined in this position paper should be subject to international monitoring, echoing the previous call of the Special Rapporteur on freedom of opinion and expression for a United Nations working group or cross-mandate task force to monitor and provide recommendations in respect of the regulation of digital surveillance.[265]

[265] A/HRC/41/35, [65] and [68].

Draft Proposed State Commitments

134. It is therefore recommended that States adopt commitments substantively equivalent to the following draft proposals:

'Each State party shall, within two years from the date of their signature, give binding domestic effect to the following obligations (whether through the enaction of domestic legislation or such other steps (if any) as are required under its national law):

134.1. *Companies domiciled within their jurisdiction are prohibited from manufacturing or offering for sale or other provision spyware technology which fails to display the following cumulative characteristics:*

(a) *Not automatically granting access to all data and/or metadata once the spyware infiltrates a network, computer, or device, and instead providing that the user must positively select the types of data and/or metadata for monitoring;*

(b) *Not automatically granting access to any data and/or metadata regarding contacts of the target network, computer, or device, and instead providing that the user must positively select any contacts for monitoring;*

(c) *Containing mechanisms to prevent harmful use, such as flagging systems and 'kill switches' in cases of apparent misuse*

(d) *Providing in all cases of use of the spyware that there is created an indelible, permanent, and uneditable auditable record of what actions have been taken by the user of the spyware, including any interferences/modifications of data/metadata, when those occurred, and by whom they were affected. This record must include a record of the producer and customer for the spyware technology, so that judicial authorities may properly be able to identify the producer and purchase of spyware used in any particular instance;*

134.2. *Companies domiciled within their jurisdiction are made subject to a binding obligation to undertake a human rights due diligence exercise upon the purchasers, and, if different, the reasonably*

foreseeable end users, of spyware technology sold. Such human rights due diligence shall be proportionate to the risk of the technology being used by purchasers, or reasonably foreseeable end users, in breach of international human rights law;

134.3. *As a separate and independent obligation, companies domiciled within their jurisdiction are made subject to a binding obligation only to sell spyware technology in circumstances where they can prove that there is no tangible risk of the technology being used by purchasers, or reasonably foreseeable end users, in breach of international human rights law;*

134.4. *For the avoidance of doubt, while the fact that such companies have obtained guarantees or assurances of compliance with international human rights law from purchasers, and/or, if different, the reasonably foreseeable end users, may be taken into account in the due diligence exercise and in the companies' assessment of the real risk of breach, the mere fact of such guarantees or assurances will not, of itself, be sufficient to demonstrate compliance with their obligations set out above;*

134.5. *As a separate and independent obligation, companies domiciled within their jurisdiction are subject to a binding obligation not to sell spyware to the agencies of any State which is not itself a signatory of this treaty;*

134.6. *Breaches of the obligations set out above are to be actionable in the ordinary domestic courts of the State on the application of persons including but not limited to persons capable of demonstrating that they are likely (subject to an appropriate evidential burden) to have been victims of breaches of international human rights law connected with the use of that companies' technology; and*

134.7. *In the event that a court determines that a breach has occurred, the persons bringing actions in respect of the same are entitled to such remedies as are available in domestic law adequately to compensate them for the violations of their international human rights which are found to have occurred.*

United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism

Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach

UNITED NATIONS
HUMAN RIGHTS
SPECIAL PROCEDURES
SPECIAL RAPPORTEURS, INDEPENDENT EXPERTS & WORKING GROUPS