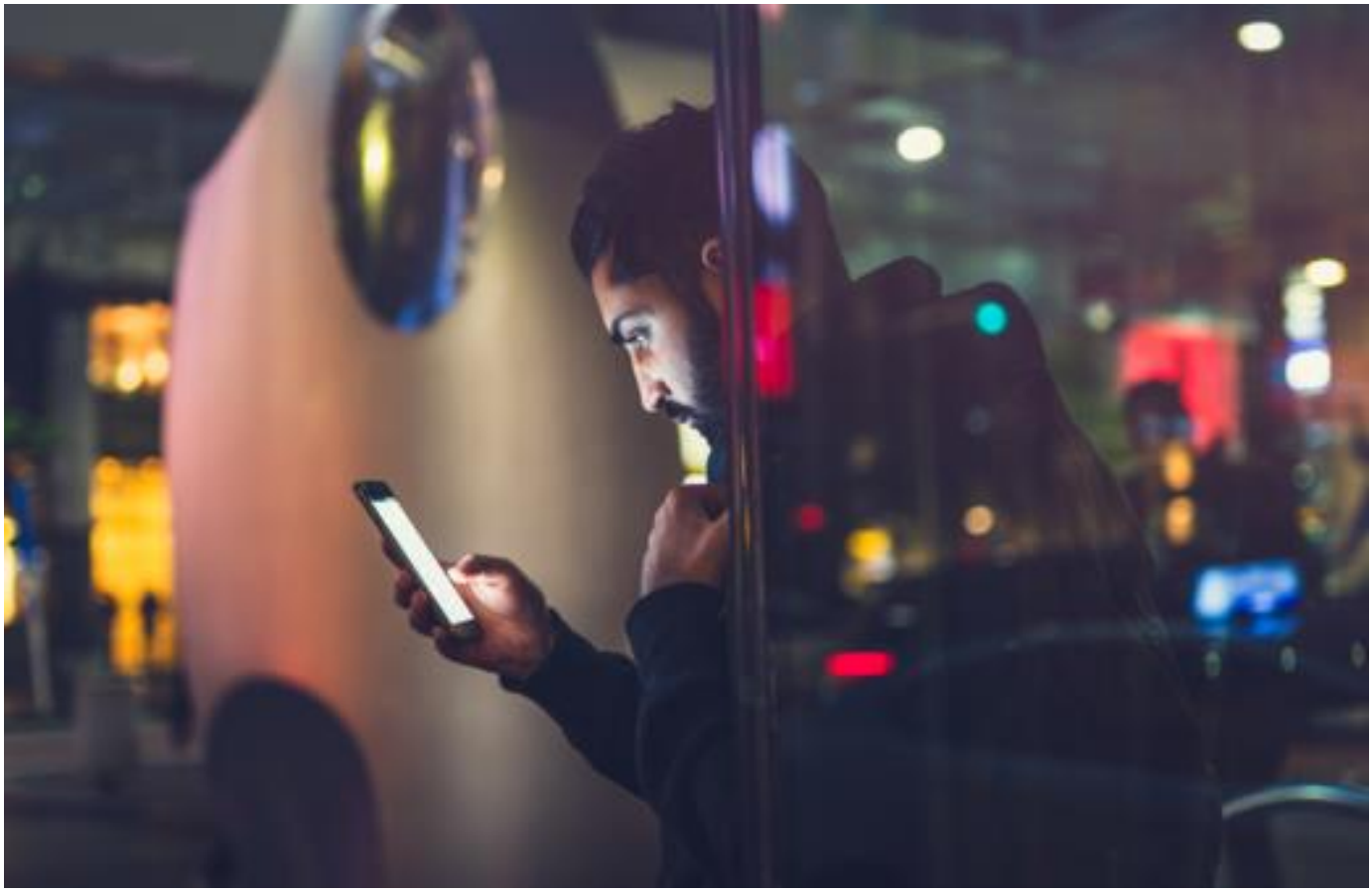

ENDING THE TARGETED DIGITAL SURVEILLANCE OF THOSE WHO DEFEND OUR RIGHTS

A SUMMARY OF THE IMPACT OF THE DIGITAL SURVEILLANCE INDUSTRY ON HUMAN RIGHTS DEFENDERS

AMNESTY INTERNATIONAL

AMNESTY INTERNATIONAL IS A GLOBAL MOVEMENT OF MORE THAN 7 MILLION PEOPLE WHO CAMPAIGN FOR A WORLD WHERE HUMAN RIGHTS ARE ENJOYED BY ALL.

Our vision is for every person to enjoy all the rights enshrined in the Universal Declaration of Human Rights and other international human rights standards.

We are independent of any government, political ideology, economic interest or religion and are funded mainly by our membership and public donations.

First published in 2019
by Amnesty International Ltd
Peter Benenson House, 1 Easton Street
London WC1X 0DW, UK

Index: ACT 30/1385/2019
Original language: English

Cover photo: *© Getty Images*

amnesty.org

AMNESTY INTERNATIONAL

CONTENTS

GLOSSARY

WORD	DESCRIPTION
MASS DIGITAL SURVEILLANCE	It is the practice of monitoring an entire population, or a significant subset of it, through digital means. It is typically done through monitoring electronic communication, digital cameras, employing facial recognition technology, collecting information through biometric databases, or even through drones, among many other tactics. While usually done by governments, it can also be implemented by private companies acting on behalf of governments or out of their own volition.
TARGETED DIGITAL SURVEILLANCE	In contrast, targeted digital surveillance is the practice of monitoring or spying on specific persons and/or organisations who may be of interest to authorities, through digital technology. Targeted digital surveillance may involve compromising devices by installing malware and spyware or compromising digital communications through phishing campaigns, among other tactics.
PHISHING	A form of cyber-attack in which fake login pages of legitimate services (such as Gmail or Facebook) are created and distributed in order to collect the usernames and passwords of the victims who are usually targeted by being sent fake links.
MALWARE	Malicious software that is designed to be secretly installed on a victim's computer or phone with the intent to steal private information or perform other forms of fraud, damage devices and/or disrupt.
SPYWARE	A particular kind of malware that is designed to stealthily spy on the victim's computer or phone and continuously monitor communications and steal private information and files.
HUMAN RIGHTS DEFENDER	Someone who, individually or in association with others, acts to defend and/or promote human rights at the local, national, regional or international levels, without using or advocating hatred, discrimination or violence.

1. A SUMMARY OF TARGETED DIGITAL SURVEILLANCE

> **"Throughout the world, conflict and fear are increasingly used to spread violence, division and silence civil society. Countries are turning their backs on solidarity and justice. Some leaders even take pride in violating human rights and are openly waging war on those who dare to stand up for what is right. As a result, the human rights defenders' movement is today confronted with an unprecedented scale of persecution and repression."**
>
> From the Human Rights Defenders World Summit, 2018.[1]

The tactics and tools of the repression carried out against human rights defenders (HRDs) with almost total impunity include personal attacks such as threats, smear campaigns, criminalization, beatings, killings, and enforced disappearances. In addition, states have also introduced a barrage of restrictions in law and practice on the rights to peaceful assembly and association, expression, and freedom of movement.

HRDs who face inequality, exclusion and discrimination, such as women, LGBTI people, migrants, black people, Indigenous communities, are doubly at risk because they are attacked not only on the basis of their struggles, but also because of who they are. The attacks they face are carried out in particular ways, have specific impacts, such as

[1] See 2018 Human Rights Defenders World Summit Website at https://hrdworldsummit.org/the-summit/#context

gender-based violence, and are often compounded by structural inequality and systematic exclusion from power and resources.[2]

These tactics have a chilling effect on the ability of HRDs to dissent, expose violations and campaign for change. We see a growing trend where states are copying each other's techniques and importing tools and technologies to apply a strategy of control and repression.

One tactic that occupies a prominent space in government playbooks across the world is that of surveillance, whether digital or otherwise. Currently digital surveillance is happening in a context where the use of technology in policing and law enforcement has expanded exponentially in recent years. In the name of fighting terrorism or maintaining law and order, governments are using a range of surveillance tactics that are impinging on the privacy of people across the world. These include tactics for both mass digital surveillance and targeted digital surveillance. Mass digital surveillance is typically done through monitoring electronic communication, CCTV monitoring, employing facial recognition technology, collecting information through biometric databases, or even through drones, among many other tactics. Countries like the **UK,**[3] **China**[4] and **USA**[5] have been reported to carry out mass digital surveillance.

In contrast, targeted digital surveillance is carried out using technologies that allow for specific targeting of persons of interest. It is carried out for example through wiretapping phones and through digital technology. It may also involve compromising devices by installing malware and spyware and interfering with digital communications through phishing campaigns, among other tactics. For instance, in the **UK**, there are reports that police have put journalists under digital surveillance,[6] in the **UAE** the government appears to have used spyware to track activists[7], in **Colombia** the national police are reported to have subjected radio journalists to digital surveillance,[8] and in **Ethiopia** the previous government used electronic surveillance to spy on opposition activists at home and abroad.[9]

With the advent of new and more sophisticated technology that is widely available, coupled with laws that restrict online freedom of expression and impinge on privacy online, the threat of targeted digital surveillance has become even more urgent.

---

[2] See Amnesty International reports: *Human Rights Defenders under threat - A shrinking space for civil society* (Index: ACT 30/6011/2017); *Deadly but preventable attacks: Killings and enforced disappearances of those who defend human rights* (Index ACT 30/7270/2019); *Laws designed to silence: The global crackdown on civil society organizations* (Index ACT 30/9647/2019) and *Challenging power, fighting discrimination – A call to action to recognize and protect women human rights defenders* (Index: ACT 30/1139/2019)

[3] See Amnesty International*, Encryption: A Matter of Human Rights* (Index: POL 40/3682/2016); Amnesty International UK, *Campaigners win vital battle against UK mass surveillance at European Court of Human Rights*, www.amnesty.org.uk/press-releases/campaigners-win-vital-battle-against-uk-mass-surveillance-european-court-human; *The UK government has been spying on Amnesty – so we're going to court*, www.amnesty.org.uk/blogs/ether/uk-government-spying-amnesty-mass-surveillance-court

[4] Information on various programmes of mass surveillance in China are available at www.hrw.org/tag/mass-surveillance-china

[5] Amnesty International, *Encryption: A Matter of Human Rights* (Index: POL 40/3682/2016)

[6] Dominic Ponsford, "Surveillance court says Met grabs of Sun reports' call records 'not compatible' with human rights law," 17 December 2015, www.pressgazette.co.uk/surveillance-court-says-met-was-right-grab-sun-journalists-call-records-hunt-plebgate-sources/

[7] Citizen Lab, 'The Million Dollar Dissident NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender', 2016, https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/)

[8] Committee for the Protection of Journalists, 'Claims police spied on two journalists revive surveillance fears of Colombia's press', 2016, https://cpj.org/blog/2016/02/claims-police-spied-on-two-journalists-revive-surv.php

[9] Amnesty International, *Encryption: A Matter of Human Rights* (Index: POL 40/3682/2016)

Countries like Thailand[10] and Bangladesh[11] have passed laws aimed at increasing the scope of electronic surveillance and giving governments intrusive powers to spy on electronic communications.

Lately, in a highly significant development, governments are contracting the services of the private digital surveillance industry to develop technology for targeted digital surveillance. These tools are then misused to unlawfully target and put human rights activists under surveillance. Companies who operate in this market have become dangerous actors responsible for creating new tools for repression and exacerbating threats against those who defend our human rights.

Little is known about this industry, which operates from the shadows despite repeated requests for more transparency. Due to weak regulatory and legal oversight, these companies can freely sell their technology to countries where human rights are not protected or respected and that in turn use the technology to track and monitor those who defend human rights.

[10] Tech Crunch, "Thailand passes controversial cybersecurity law that could enable government surveillance", 28 Feb 2019, https://techcrunch.com/2019/02/28/thailand-passes-controversial-cybersecurity-law/ and Reuters, "Thailand defends cybersecurity law amid concerns over rights abuse", 1 Mar 2019, WWW.REUTERS.COM/ARTICLE/US-THAILAND-CYBER/THAILAND-DEFENDS-CYBERSECURITY-LAW-AMID-CONCERNS-OVER-RIGHTS-ABUSE-IDUSKCN1QI4KA

[11] Amnesty International 'Bangladesh: New Digital Security Act is attack on freedom of expression', November 2018, www.amnesty.org/en/latest/news/2018/11/bangladesh-muzzling-dissent-online/

2. TARGETED DIGITAL SURVEILLANCE AND THE SHRINKING SPACE FOR DISSENT

The targeting of human rights defenders because of their work using digital surveillance technology is unambiguously illegal under international human rights law. Unlawful surveillance violates the right to privacy and impinges on the rights to freedom of expression and opinion, of association and assembly. Both the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (ICCPR) protect these rights. The Covenant upholds the right to hold opinions without interference[12] and guards against arbitrary and unlawful intrusion of their privacy.[13] International law and standards also require that any interference by the state on the right to privacy should be lawful, necessary, proportional, and legitimate. States are also required to ensure that individuals whose rights have been violated have access to remedy.[14]

It is often virtually impossible for human rights defenders to prove the existence of surveillance, either because of technical hurdles or because its use is covert.[15] Even where targeting or the presence of an active infection cannot be proven,[16] the fact of living under the constant threat of *possible* surveillance may constitute a human rights violation in itself.[17]

---

[12] Article 19, International Covenant on Civil and Political Rights
[13] Article 17, International Covenant on Civil and Political Rights
[14] Article 2(3), International Covenant on Civil and Political Rights
[15] Amnesty International, *Human Rights Defenders Under Threat - A Shrinking Space for Civil Society (Index*: ACT 30/6011/2017)
[16] 'Targeting' refers to when an attempt has been made to put someone under surveillance. This can be done by sending malicious links containing spyware, or by any other means. This may or may not be successful. However, when targeting is successful devices of the user may be infected and compromised.
[17] Amnesty International, *A Dangerous Alliance: Governments Collaborate with Surveillance Companies to Shrink the Space for Human Rights Work,* (Blog, 16 August 2019)

Regardless of whether the attempt at surveillance is successful or not, targeting of human rights activists instils fear and has a chilling effect on their ability to continue their work without undue interference.[18] In many instances this leads those who defend human rights to self-censor and refrain from exercising their rights to freedom of expression, association and peaceful assembly. This is compounded by having to fight malicious prosecutions through information that is extracted, misused and manipulated, diverting human rights defenders' energy and resources to fighting judicial proceedings.[19] The threat of surveillance may have a detrimental effect on the mental health of human rights defenders and information may be used to divulge details in the public sphere exposing them personal attacks and smear campaigns. All of this has a damaging knock-on effect on communities and societies whose rights HRDs are fighting for.

For example, in **Azerbaijan**, human rights activists under the constant threat of surveillance who leave their homes due to fear of attacks, find it hard to communicate with their loved ones back at home, worrying that they too will be targeted.[20] In **Uzbekistan**, those who have been targeted by cyber-attacks and have left their homes, have remained the targets of digital surveillance campaigns.[21] This effectively means that human rights defenders have had to live in a constant state of fear, perpetually looking over their shoulders and feeling a sense of impending danger wherever they go. Surveillance is a highly effective way of discouraging or preventing those who defend human rights from dissenting and exposing violations.[22]

[18] Global Justice Clinic, NYU School of Law, *Attempted digital surveillance as a completed human rights violation: Why targeting human rights defenders infringes on rights. Submission to the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 1 March 2019, https://chrgj.org/wp-content/uploads/2019/05/190301-GJC-Submission-on-Surveillance-Software.pdf

[19] See Amnesty International *'Laws Designed to Silence: The Global Crackdown on Civil Society Organizations* (Index: ACT 30/9647/2019)

[20] Amnesty International, 'False Friends: How Fake Accounts and Crude Malware Targeted Dissidents in Azerbaijan', (Blog, 9 March 2017)

[21] Amnesty International, "*We Will Find You Anywhere" -The Global Shadow of Uzbekistani Surveillance* (Index: EUR 62/5974/2017)

[22] Amnesty International, *Human Rights Defenders Under Threat - A Shrinking Space for Civil Society* (Index: ACT 30/6011/2017)

3. CASE STUDY: CYBER ATTACKS AGAINST PAKISTANI HRD DIEP SAEEDA

> **"Every time I open an email I am now scared. It's getting so bad I am actually not able to carry out my work – my social work is suffering."**
>
> Diep Saeeda[23]

In 2018, Diep Saeeda, a prominent Pakistani woman human rights defender was actively campaigning to seek accountability for the enforced disappearance of another Pakistani defender, Raza Khan. During this time, Diep became the target of a concerted cyber-attack campaign. One Facebook user who claimed to be an Afghan woman named Sana Halimi, living in Dubai and working for the UN, repeatedly contacted Diep Saeeda via Facebook Messenger saying that she had information about Raza Khan. The operator of the profile sent Diep links to files containing malware called 'StealthAgent' which, if opened, would have infected her mobile devices. The profile, which Amnesty International believes was fake, was also used to trick Diep into divulging her email address, to which she started receiving emails infected with a Windows spyware commonly known as 'Crimson RAT'.

Diep Saeeda also received emails claiming to be from staff of the Chief Minister of Punjab province. The emails included false details of a supposed upcoming meeting between the provincial Ministry of Education and Diep's organization, the Institute for Peace and Secular Studies. In other instances, the attackers pretended to be students looking for guidance. Amnesty International was able to establish that other defenders in Pakistan were also targeted in similar ways.

---

[23] Amnesty International, *Pakistan: Human Rights Under Surveillance* (Index: ASA 33/8366/2018)

The cyber-attack made it difficult for Diep Saeeda to carry out her work and she began to live in fear. She began distrusting e-mails and attachments even from her family members, fearing that someone might be impersonating them.

4. THE PRIVATE DIGITAL SURVEILLANCE INDUSTRY

A number of governments purchase digital surveillance tools - particularly spyware - from commercial surveillance companies. These are then used to track, monitor and intimidate human rights defenders, and others who dissent. Both the governments and the companies selling it to them claim that the technology is only used for lawful purposes, such as watching and tracking terrorists and criminals. However, mounting evidence of their misuse tells a different story. Civil society organizations, including Amnesty International, have uncovered targeted campaigns against those who defend human rights with technology that is marketed by many of these surveillance companies.

While governments have been producing spyware for some time now, commercial spyware is relatively new but equally invasive and sophisticated.[24] Companies such as NSO group in **Israe**l and **Luxembourg**[25] and Finfisher in the **UK** and **Germany**[26] are just some of the key players in this secretive and highly profitable industry.

According to Citizen Lab, just one of these, the NSO group, appears to have been behind known targeted surveillance attacks in at least 45 countries.[27] In June 2018, an Amnesty International staff member received a malicious WhatsApp message with **Saudi Arabia**-related bait content and carrying links that could have installed mobile spyware manufactured by the NSO group.[28] Many of the countries that have been able to buy surveillance technology from these companies have a dismal human rights

[24] Just Security, 'CTRL+HALT+Defeat: State-sponsored Surveillance and the suppression of Dissent', by Julie Bloch, Sukti Dhital, Rashmika Nedungadi and Nikki Reisch, 15 May 2019, www.justsecurity.org/64095/ctrlhaltdefeat-state-sponsored-surveillance-and-the-suppression-of-dissent/

[25] Business and human rights resource centre, "Amnesty backs legal action against Israel firm NSO group over spyware used against human rights defenders", May 2019, www.business-humanrights.org/en/amnesty-backs-legal-action-against-israeli-firm-nso-group-over-spyware-use-against-human-rights-defenders

[26] Amnesty International, "New tool for spy victims to detect government surveillance" (News , 20 November 2014)

[27] Citizen Lab, 'HIDE AND SEEK. Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries', September 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

[28] Amnesty International, *Amnesty International among targets of NSO-powered campaign'*, 1 August, 2018, www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/

record. For instance, NSO group's software has been used to attack human rights defenders in **Morocco,**[29] **Mexico, Saudi Arabia, and UAE.**[30]

Companies like the NSO group have a responsibility under the UN Guiding Principles for Business and Human Rights to ensure a robust due diligence process to prevent the use of their products from violating human rights and to mitigate and remedy such abuse.[31] Further, states have a responsibility to protect against private entities violating human rights, regardless of whether these violations occur within their borders or outside them.

Demanding accountability from these companies that are shrouded in secrecy is particularly difficult. Very often, they hide behind arguments of 'security considerations' or 'confidentiality clauses' to keep information on their activities out of the public domain. Little is known about these companies or their corporate structures. Many of them do not disclose data on export licensing contracts and have either no provisions for conducting human rights due diligence and remedy for abuses or have entirely unsatisfactory ones. This, coupled with a lack of regulatory oversight and weak export licensing frameworks at both the domestic and international levels, has made the task of confronting this industry challenging.

For instance, instruments like the Wassenaar Arrangement, a multilateral arrangement on export controls, are designed to harmonise export rules among participating states with regards to military and dual-use goods and technologies which contribute to military capabilities.[32] While the arrangement may be useful, it is not a forum designed to mitigate human rights concerns.

Domestic export licensing regimes, like that of Israel[33] and other countries, have a record of approving export licenses despite human rights concerns, as strategic considerations often outweigh human rights ones. The European Union does have clearer human rights frameworks, but member states nevertheless also continue to approve licenses for surveillance technology despite concerns and evidence of previous abuses which should lead to licenses being denied.[34] At the same time, secrecy provisions undermine companies' ability to meet their own human rights obligations under different jurisdictions.

All this leaves a legal and regulatory vacuum that allows the sale and transfer of digital surveillance technology without adequate safeguards. The longer these companies and the states that buy technology from them evade scrutiny, the more the space for dissent and human rights defense shrinks dangerously. We need to urgently

---

[29] Amnesty International, 'Morocco: Human Rights Defenders Targeted with NSO Group's Spyware', 2019 www.amnesty.org/en/latest/research/2019/10/morocco-human-rights-defenders-targeted-with-nso-groups-spyware/
[30] Citizen Lab, 'HIDE AND SEEK. Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries', September 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/
[31] UN Guiding Principles on Business and Human Rights, www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf
[32] www.wassenaar.org/the-wassenaar-arrangement/
[33] Amnesty International, *Amnesty International affidavit in support of Israeli petition,* (Index: ACT 10/0332/2019) and 'Israel: Amnesty International engages in legal action to stop NSO Group's web of surveillance', (News, 13 May 2019)
[34] Amnesty International, 'EU: States push to relax rules on exporting surveillance technology to human rights abusers', (News, 11 June 2018)

end these surveillance attempts by states that unlawfully employ privately manufactured surveillance equipment to target human rights activists.

5. HUMAN RIGHTS OBLIGATIONS OF STATES AND COMPANIES

At the international, regional and national level, a number of instruments outline the obligations to respect and protect HRDs. States have an obligation to uphold these standards in order to guarantee a safe and enabling environment in which HRDs can work free from fear of attack and pursue their crucial work for the protection and promotion of all human rights.[35]

The UN Declaration on Human Rights Defenders (1998)[36] is based on existing binding international instruments. The Declaration reaffirms the right to defend human rights and articulates states' obligations to the particular role and situation of HRDs. It outlines the related responsibilities and duties of states and makes clear that it is states that bear the ultimate responsibility to protect HRDs, to prevent and effectively address allegations of human rights violations and abuses committed against them, and to ensure that they can carry out their work in a safe and enabling environment. Moreover, the Declaration highlights the critical role of human rights defenders in making the human rights a reality, as well as to develop and discuss new human rights ideas and principles, and to advocate their acceptance.

Nation states have binding obligations under international human rights law to protect human rights from abuse by third parties. This includes the obligation to regulate the conduct of non-state actors who are under their control in order to prevent them from causing or contributing to human rights violations, even if they occur in other countries.

As laid out in the UN Guiding Principles on Business and Human Rights (UNGPs)[37], companies also have a responsibility to respect human rights wherever they operate in the world. The UNGPs require that companies take pro-active steps to ensure that they do not cause or contribute to human rights abuses within their global operations, and to respond to any human rights abuses when they do occur. In order to meet that responsibility, companies must carry out human rights due diligence to "identify, prevent, mitigate and account for how they address their human rights impacts." The

[35] Amnesty International, *Amnesty International Comments on the European Commission Dual-Use Export Proposal* (Index POL 10/1558/2017)
[36] Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms, 1998, UN Doc. A/RES/53/144
[37] UN Guiding Principles on Business and Human Rights, www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

corporate responsibility to respect human rights exists independently of a state's ability or willingness to fulfil its own human rights obligations and over and above compliance with national laws and regulations protecting human rights. For example, the interpretative guidance on the UNGPs specifically notes that a company may contribute to a human rights violation if it provides "data about Internet service users to a Government that uses the data to trace and prosecute political dissidents contrary to human rights."[38]

Moreover, it is possible that a company that sells surveillance equipment could be complicit in any subsequent violation of human rights in which the equipment is used. An International Commission of Jurists (ICJ) Panel of Experts has examined the question of corporate complicity in human rights violations in some depth and clarified how legal liability, both civil and criminal, could arise for such complicity. The ICJ panel considered that there could be a sufficiently close link in law if the company's conduct enabled, exacerbated or facilitated the abuse, and the company knew, or ought reasonably to have known, that the abuse would occur, and that crucially a company could enable, exacerbate or facilitate abuse through, among other things, the provision of goods or services.[39]

[38] OHCHR, *The Corporate Responsibility to Respect Human Rights: An Interpretive Guide*, 2012, p.17, www.ohchr.org/Documents/Publications/HR.PUB.12.2_En.pdf

[39] ICJ, *Report of the ICJ Expert Legal Panel on Corporate Complicity in International Crimes*, 2008, www.icj.org/report-of-the-international-commission-of-jurists-expert-legal-panel-on-corporate-complicity-in-international-crimes/

6. RECOMMENDATIONS

> **"States should impose an immediate moratorium on the export, sale, transfer, use or servicing of privately developed surveillance tools until a human rights-compliant safeguards regime is in place."**
>
> UN Special Rapporteur on Freedom of Expression, David Kaye[40]

States bear the ultimate responsibility to protect human rights defenders, to prevent and effectively address allegations of human rights violations and abuses committed against them or their human rights work, and to ensure that they can carry out their work in a safe and enabling environment. Much is left to be done to recognize and protect all those who speak out and stand up against injustice and to protect them from targeted digital surveillance.

6.1 STATES

Amnesty International calls on all states to:

- Implement a moratorium on the sale and transfer of surveillance equipment until a proper human rights regulatory framework is put in place
- Disclose information about all previous, current, or future contracts with private surveillance companies by responding to requests for information or by making proactive disclosures
- Deny export authorization where there is a substantial risk that the export in question could be used to violate human rights – either through unlawful surveillance or where the destination country has inadequate legal, procedural and technical safeguards in place to prevent abuse
- Ensure that all relevant technologies are scrutinized prior to transfer
- Ensure transparency regarding the volume, nature, value and destination of surveillance transfers
- Ensure that encryption tools and legitimate digital security tools are not subject to export controls
- Implement domestic legislation that imposes limits on digital surveillance, ensuring that:
    - Surveillance is governed by precise and publicly accessible laws

[40] OHCHR, Surveillance and human rights, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc. A/HRC/41/35, 28 May 2019

    - Surveillance is only against specified persons, authorized by a competent, independent and impartial judicial body with limitations on time, manner, place and scope of surveillance
    - Authorized digital surveillance is subject to detailed record keeping, in accordance with documented legal processes for a warrant, and targets are notified as soon as practicable without jeopardizing the purpose of surveillance
- Ensure that all digital surveillance is subject to public oversight mechanisms, including:
    - An approval process
    - Public notice and consultation for new surveillance purchases
    - Regular public reporting
- Ensure adequate mechanisms for domestic legal redress in cases of unlawful and/or abusive targeted digital surveillance.

6.2 BUSINESSES

Amnesty International urges businesses to:

- Publicly commit to respecting human rights, and the work and security of human rights defenders
- Implement adequate human rights due diligence processes, as set out in international business and human rights instruments, such as the UN Guiding Principles on Business and Human Rights and the OECD Guidelines for Multinational Enterprises, to ensure their activities, or those of their subsidiaries, sub-contractors and suppliers respect the rights of HRDs and do not hinder their legitimate work
- As part of their responsibility to conduct human rights due diligence, companies should carry out robust human rights risk assessments for all proposed transfers, which should in turn be scrutinized by export authorities, and made public
- Ensure transparency with regard to sales and contracts
- Conduct consultations with rights holders before signing contracts in countries
- Implement contractual protections against human rights abuses
- Implement design and engineering choices that incorporate human rights standards
- Ensure regular audits into verification processes, the results of which are publicly disclosed
- Have an adequate notification process for reporting misuse of technology and grievance mechanisms
- Implement robust mechanisms for compensation of targets of unlawful surveillance or other forms of redress.

6.3 INVESTORS

Amnesty International urges all investors to:

- Investors should ensure that they don't contribute to human rights violations by way of their stake in surveillance companies. They should do this by demanding robust transparency and human rights due diligence from surveillance companies
- Investors should communicate the applicable aforementioned recommendations to the surveillance companies they have stakes in and call for their implementation.

AMNESTY INTERNATIONAL IS A GLOBAL MOVEMENT FOR HUMAN RIGHTS. WHEN INJUSTICE HAPPENS TO ONE PERSON, IT MATTERS TO US ALL.

CONTACT US


info@amnesty.org


+44 (0)20 7413 5500

JOIN THE CONVERSATION


www.facebook.com/AmnestyGlobal


@Amnesty

INDEX: ACT 30/1385/2019
DECEMBER 2019
LANGUAGE: ENGLISH

amnesty.org