U4 Helpdesk Answer

U4 Helpdesk Answer 2023:7

The implications of spyware and surveillance technology for anti-corruption activists

The capabilities of modern surveillance software allow for the monitoring and tracking of people on a mass and automated scale. Recent trends include "zero click" technology that allows spyware to be downloaded onto a device without the need for the victim to click on a link, and then provides unfettered access to the device's camera, microphone, and other personal data. This unprecedented level of intrusion has been condemned as a breach of fundamental human rights, such as freedom of expression and privacy.

Currently, there is little transparency regarding the development and acquisition of these technologies. Studies show that technology companies developing surveillance software are just as likely to sell this software to autocratic states and criminals as they are to democratic governments. This is a concern as authoritarian regimes frequently claim that journalists, dissidents and human rights activists are criminals or a national security threat to justify subjecting them to intrusive surveillance. Where civil society groups are targeted and intimidated by spyware, it reduces their capacity to hold governments to account and investigate cases of corruption, and it can lower political participation and undermines democracy.

22 March 2023

AUTHOR
Caitlin Maslen (TI)
tihelpdesk@transparency.org

REVIEWED BY
Andrea Rocca and Matthew Jenkins (TI)

Pauline Lemaire (CMI)

RELATED U4 MATERIAL

↗ Biometric data: putting people at risk in the name of anti-corruption

Query

Please provide a summary of the corruption risks and threats of surveillance malware, particularly when it is used against anti-corruption activists. What can be done to mitigate these risks?

Contents

1. Background
2. Examples of surveillance malware
3. Opportunities for corrupt practices
    a. The development and acquisition of surveillance malware
    b. The deployment of surveillance malware
    c. Case studies
4. Development projects and surveillance malware
5. Risk mitigation of surveillance malware
    a. The role of civil society
    b. Strengthening export controls
    c. Increasing regulation and oversight of the use of surveillance software
    d. Promoting integrity in technology companies that develop surveillance software
    e. The role of international donors
6. References

MAIN POINTS

- Spyware is increasingly being deployed against civil society and journalists to monitor, intimidate them, and this can even lead to physical confrontations and arrests.
- Surveillance also creates the pre-conditions for corruption through reducing accountability, political participation, and narrowing civic space.
- Further regulatory controls can ensure that surveillance software is not used to illicit means, such as the EU's Dual-use export control (2021) and the Wassenaar Arrangement.
- Civil society also has an important role in ensuring surveillance software is not deployed for corrupt means, through their investigations, advocacy and close collaborations with the cyber security industry.

Caveat

Emerging technologies play an important role in measures to counter corruption. Open-source data, artificial intelligence and the blockchain, have been used to expose corruption and deter officials from committing corrupt acts (Adam and Fazekas 2021). Surveillance software has made tracking and monitoring of terrorists and criminals more effective and efficient. While acknowledging these potential benefits, this Helpdesk Answer focuses on the threats and risks associated with surveillance software. A careful balance needs to be struck between the technology's benefits to society and democracy and ensuring it does not curtail

freedoms of expression and privacy, human rights, or even create opportunities for corrupt acts.

Background

The scope and variety of surveillance now available is unprecedented in human history (Richards 2013). Today, it is possible to monitor and track an individual or group's location, communications, browsing history (and more) on a mass scale. It has been said that we are currently living through the "age of surveillance" (Richards 2013).

This amount of surveillance has been enabled by recent leaps in the capabilities of digital technology and spurred on by global events such as the Covid-19 pandemic (MENA Rights Group 2020). Surveillance software is used to track and monitor individuals and groups through infecting devices such as computers, smartphones, cameras, drones, as well as biometric data with malware (Privacy International 2018). In recent decades, technological capabilities have rapidly accelerated, leading to the emergence of a large surveillance software industry comprising of state and private owned companies that sell products to clients that can include governments and law enforcement agencies (Privacy International no date b).

Surveillance software includes ICT goods, services, and technologies that are "specifically designed in whole or in part for surveillance purposes" (Access Now 2022a). These can be used for mass surveillance which is indiscriminate and collects data on large numbers of individuals, or for targeted surveillance which is directed at individuals (Access Now 2022a).

Spyware (otherwise known as surveillance malware), which this Helpdesk Answer focuses on, is an example of targeted surveillance that is deployed for deceptive and hidden means. "Malware" is short for "malicious software" and refers to programs that are designed to conduct unwanted actions on a device (SSD no date). These unwanted actions typically mean that the software has been installed on an individual's device without their consent and is tracking their communications and other data points without their knowledge.

Because surveillance software (and malware/spyware) can be used both for civilian and military purposes, it is considered a dual-use product. Dual-use exports can contribute to international peace (EU no date) but are also high risk to human rights and security if not regulated correctly (Alam and Chantsoz 2016).

Moreover, surveillance software transcends the public and private divide, and the relationship between governments and private technology companies developing surveillance software is complex (Richards 2013). As seen with many dual-use goods, the two are intertwined and use the same technologies and techniques through private and public partnerships (Richards 2013).

In recent years, several scandals have come to light of governments and enforcement agencies using surveillance malware to track journalists, activists, political opponents and other individuals without their consent, knowledge and purely on account of their work. The most notable of these was the 2021 Pegasus spyware scandal, which was uncovered through a collaborative effort of journalists, civil society organisations (CSOs) and activists. While surveillance software and spyware can be used to track terrorists and criminal groups, cases such as Pegasus show that its use against civil society can pose a threat to individual security, civil society, human rights, and democracy itself (Privacy International 2018).

Spyware is a powerful tool that can undoubtedly be abused for corrupt purposes. Corruption is "the abuse of entrusted power for private gain" (Transparency International no date). When governments deploy spyware against civil society activists, this constitutes an abuse of their entrusted power for private gain, in the sense that it helps them consolidate their political power by neutering legitimate opposition.

The improper use of spyware on legitimate civil society groups reduces democratic accountability by curtailing the ability of activists to hold governments to account and raises questions about the integrity of public officials who make use of these technologies. Ultimately it can serve to reduce citizen participation and thus increase the opportunities for governments to act with impunity (Schächtele et al. 2022). Worryingly, it is not only authoritarian governments that have deployed spyware against civil society; democratic states are also increasingly acquiring and using spyware on their citizens (Richards 2013: 1936).

This Helpdesk Answer looks at the different types of spyware that have been used against civil society as well as the corruption risks that have emerged because of this. It focuses on examples of spyware being deployed against activists, journalists and civil society as well as development and humanitarian aid organisations. Finally, solutions to mitigate the corruption risk posed by these new technologies are discussed. These include better regulation of the industry, increased safeguards on government use and empowerment of civil society to protect themselves and expose the illicit and corrupt use of spyware by governments.

Examples of surveillance malware

The surveillance software industry has rapidly expanded in recent years. Technology companies developing surveillance software sell their technology to law enforcement and intelligence agencies for compliance and security purposes (Privacy International 2018). The number of state-owned surveillance technology companies has also risen, such as China's Hikvision and Dahua Technology (Big Brother Watch Team 2022).

The technologies produced and sold by these companies include small GPS tracking devices, cameras, hidden transmitters, as well as more sophisticated systems such as equipment that monitors internet communications on a nationwide scale technology (Privacy International 2018). The software can also be used to collect biometric data, which includes fingerprints, iris scans, facial images and other personal data such as residence, occupation, religion, family and any other data on a device including the apps, contact list, photos, call log, among others (Aarvik 2022). Spyware specifically includes targeted surveillance technology that remotely activates cameras, microphones, and intercepts communications to receive personal data such as calendar invite, passwords, contacts list, among others (Access Now 2022a).

Social media platforms are also a source of personal data for surveillance malware as they contain information on the user's personal preferences, political and religious views, physical and mental health and identity of their friends and families (Privacy International no date b). Software can be used to collect information from social media platforms with the intention to monitor their networks, profile and manipulate these people and

groups (Privacy International no date b). Both democratic and authoritarian governments have been recorded using this form of surveillance (Privacy International no date b).

Spyware that has been deployed against civil society includes the same features as those sold for compliance and national security objectives. One example is the Italy based Hacking Team's Remote-Control Systems (RCS) spyware that was sold to governments and consists of sophisticated computer spyware (Marczak et al. 2014). The RCS spyware relies on obfuscating methods that make it difficult to identify who is using the software once the surveillance is detected and is therefore considered untraceable (Marczak et al. 2014). Leaked documents suggested that Hacking Team's clients included the governments and security services of Azerbaijan, Kazakhstan, Uzbekistan, Russia, Bahrain, Saudi Arabia and the UAE. Many of these governments have been criticised for their surveillance of citizens, activists and journalists, both domestically and overseas (Hern 2015).

Another example of spyware technology is the Israel based NSO Group's Pegasus software. This spyware is considered one of most advanced tools available and uses "zero-click" technology to be deployed and installed onto a computer or smartphone, which heightens the sense of uncertainty of whether someone is being subjected to surveillance or not (Global Justice Clinic 2019). It involves an SMS message sent to the target, and no clicks to hyperlinks are needed for the spyware to be remotely installed and collect data on the individual (Global Justice Clinic 2019). The data harvested includes SMS, emails, photos, videos and contact details, and the spyware can also record calls, activate the microphone and camera, and collect GPS data (Corera 2021). The NSO Group claimed they only sold their spyware to governments to use it against criminals and terrorists, but leaks showed that it was deployed against civil society activists and journalists in multiple countries (Corera 2021).

The number of surveillance technology manufacturers that produce spyware is growing, and the majority of these are registered in the EU, the US, China and Israel (Schächtele et al. 2022; Miyamoto 2020). The digital rights organisation Privacy International found that Germany and Europe in general are among the top players and are as likely to supply their products to western intelligence agencies as to autocratic leaders (Schächtele et al. 2022).

Opportunities for corrupt practices

The development and acquisition of surveillance malware

There is very little transparency on the procurement and acquisition of spyware, despite their clients often being government agencies (Privacy International 2016: 56). Technology companies that develop spyware are notoriously opaque about their operations and unresponsive to those who reach out for more information.

For example, Access Now reported that, together with CSOs, they attempted to contact technology companies that develop surveillance software about their spyware in Latin America, particularly those that have been deployed against human rights defenders, but no companies responded to their requests (Alarcón 2022). The only data available on their acquisition is from investigative reporting and some data published by a small number of governments. Together, this indicates that a wide

range of government agencies are purchasing this software, including in some of the most authoritarian countries in the world (Privacy International 2018).

As an example, in 2017, the Trojan software[1] Finspy, from the Munich based company FinFisher, was found on websites in Turkey. The sites pretended to be part of the Turkish opposition movement and asked activists to download a networking app, which then secretly installed the surveillance programme using Trojan software (Schächtele et al. 2022). There was little transparency around who acquired this software which targeted activists from the opposition movement.

The scale at which government and law enforcement agencies are acquiring surveillance technologies is slowly coming to light. For example, the ACLU in California has received thousands of pages of public records that show that law enforcement agencies have secretly acquired social media spying software (Ozer 2016). The potential uses of this include the surveillance of activists. The researchers requested records from 63 police departments, sheriffs, and district attorneys across the Californian state, and learned that 40% of all police departments had acquired social networking surveillance tools (Ozer 2016). While the technology sold in this case is social media spying software, the procurement processes of this and other dual-use spywares are similarly opaque.

As noted in the literature, limitations (such as procurement transparency standards) that are placed on the public sector do not always apply to the private sector (Miyamoto 2020: 55). When private surveillance companies work closely with governments the boundaries are unclear (Miyamoto 2020: 55). Indeed, the UN Human Rights Council has observed that the "private [digital surveillance] industry has stepped in, unsupervised and with something close to impunity" (Human Rights Council 2019).

This lack of transparency on the public procurement processes can open for corrupt practices when public entities acquire spyware. Companies can skirt export regulation to benefit from fraud and violate customs regulations (Benjajkob, Breinder, Scharf 2023). For example, a recent investigation into an Israeli cyber offense firm that sells spyware to foreign countries showed that it was exporting sensitive technologies without obtaining the requisite Defense Ministry license (Benjajkob, Breinder, Scharf 2023).

The deployment of surveillance malware

Spyware is increasingly being deployed to monitor and track citizens, civil society, and journalists; thereby reducing the ability for society to hold government to account. Such use of spyware against citizens and civil society curtails fundamental human rights. When these groups are targeted and intimidated by spyware, it reduces their capacity to hold governments to account and investigate cases of corruption, and it lowers political participation, and undermines democracy.

Indeed, this increased surveillance of internet behaviour has led to more arrests and prosecutions of activists and civil society actors (Tactical Tech no date). It affects the freedom of expression of

[1] Trojan software is a type of malware that downloads onto a computer disguised as a legitimate program, typically hidden as an attachment in an email or a free-to-download file which then transfers onto the user's device (Fortinet no date).

politically engaged actors and limits their political participation (Tactical Tech no date). Not only are local NGOs and CSOs targeted but so are larger international organisations and actors such as Greenpeace and Amnesty International, and by states that are typically considered democratic (Tactical Tech no date). Ultimately, this compounds the trend of a shrinking civic space that has been, in recent years, observed throughout the world (CIVICUS Monitor 2020).

Moreover, recent spyware such as that deployed by the US National Security Agency (NSA), which activates microphones and records private conversations, allows for intrusion and data collection of an unprecedented scope and depth (Edward-Gill, Köbis and Starke 2022). This infringes on the right to privacy and prevents the exercise of freedom of opinion and expression (Global Justice Clinic 2019).

This infringement of human rights and reduction in government accountability is seen in the growing prevalence of protest surveillance. This involves deployment of surveillance tools (beyond that of just spyware), and the acquisition, processing, analysis and use of information about people engaging in protests, whether or not they are suspected of any wrongdoing (Privacy International no date a). For example, state and local police departments used invasive smartphone surveillance devices that mimic cellphone towers to trick cellphones in the area to transmit their location and identifying information to gather information from protesters (ACLU 2018; Zetter 2020). Like the use of covert spyware, this potentially affects human rights, right to privacy, political participation and freedoms of assembly and expression (Privacy International no date a).

Xu Xu (2021) studies the consequences of large-scale digital surveillance in authoritarian states. Using a sample of three thousand Chinese countries and districts to examine how digital surveillance influences government repression and co-optation, they find that surveillance for identifying individual opponents results in more repression and less redistribution (Xu Xu 2021). It does so through resolving the dictator's information problem of not knowing individual citizens' true anti-regime sentiments and allows them to target their repression to forestall coordinated uprisings (Xu Xu 2021). Xu Xu finds that surveillance increases local governments' public security expenditure and arrests of political activists but decreases public goods provision (Xu Xu 2021). Therefore, they conclude that the use of mass surveillance makes citizens' lives worse off in dictatorships.

Moreover, even when deployed in democratic states, the mass use of surveillance technology and spyware goes against the beliefs and values that the citizens expect from their governments, and therefore undermines democratic political culture (Miyamoto 2020). And, in the future as more data becomes available, governments may outsource some digital analysis and investigation to the private sector, which will cause additional security related issues (Miyamoto 2020: 56). For example, this could mean that a private company could use the insider policing information for profit (Miyamoto 2020: 56).

The lines between who can be surveilled and who cannot be are increasingly blurred. Many authoritarian countries frequently claim that journalists, dissidents and human rights activists are criminals or a national security threat making them worthy of intrusive surveillance (Corera 2021). Indeed, most experts agree that, barring some form of political intervention, surveillance capitalism (where personal data is commodified and increasingly collected for profits) will continue to exacerbate trends of rising social and wealth inequality (Zuboff 2015).

The deployment of surveillance software by police has brought legal problems in many jurisdictions. For example, in 2022, a constitutional complaint was brought to Germany's top court by the German Society for Civil Rights (GFF) complaining that surveillance tools are being used to create profiles of suspected criminals before any crimes have been committed (Knight 2022). In response, the state government argued that the program does no more than coordinate data that it has already gathered from other sources (such as surveillance cameras and online public records) and is vital to preventing serious crimes (Knight 2022). While the technology in question was not spyware, the lines between what constitutes spyware and surveillance software are often blurred and can raise similar legal and ethical dilemmas.

Case study: Targeting foreign CSOs

The deployment of surveillance, particularly when this surveillance is of individuals in other countries, can create an environment of conflict and political tension, and may even lead to retaliatory measures (Alam and Chantzos 2016). For example, six Palestinian CSOs were targeted by the NSO Group's Pegasus spyware, a fact uncovered in 2021 after the organisations contacted Front Line Defenders with the suspicion that their devices had been infected (Front Line Defenders 2021). Prior to this, the Israeli Minister of Defence had announced that these six CSOs were designated as "terrorist organisations" under Israel's Anti-Terrorism Law 2016.

By designating them terrorist organisations, it gave Israeli authorities the power to seize their assets, arrest their staff members and interfere with international donor funding (Front Line Defenders 2021). At the same time, they were being subject to surveillance by the Pegasus technology, showing a continuation and escalation of Israel's violation of Palestinian citizen rights (CIVICUS 2022).

Case study: Targeting investigative journalists

Several investigative journalists in Uganda were reportedly targeted by the Pegasus spyware, including those working at NBS Television and NTV Television (Kirabo 2021). The journalists discovered the infection after receiving a notification from Apple saying that "state-sponsored attackers may be targeting [this] phone" (Kirabo 2021). The targeted journalists stated that they did not know why they were being monitored by the spyware (Kirabo 2021).

Case study: Hacking the phones of family members of a government critic

The phone of Belgian citizen, who is the nephew of Paul Rusesabagina, a jailed critic of the Rwandan government, was reportedly hacked several times in 2020 by the Pegasus spyware (Kirchgaessner and Taylor 2022). Findings by Citizen Lab also show that the daughter of Rusesabagina, who is a dual American-Belgian national, was also targeted by the Pegasus spyware.

It has been suggested that these reports show that the Rwandan government deployed a surveillance campaign against the family of Rusesabagina during the time that some of them were in discussions with EU and US officials about the activist's arrest, trial, and imprisonment (Kirchgaessner and Taylor 2022). Furthermore, the US state department has classified Rusesabagina's case as "wrongful detention" and have claimed that Rwandan officials have also targeted the phones of other US-based Rwandan dissidents (Kirchgaessner and Taylor 2022).

Case study: Intimidation of journalists reporting on corruption

Two journalists who report on corruption were infected by NSO Group's spyware in 2021 in Mexico, according to the digital rights researchers at Red en Defensa de los Derechos Digitales and the Citizen Lab (Kirchgaessner 2022). One of the journalists had been reporting on corruption and the relationship between the Mexican government and cartels, and their device was infected after writing about extrajudicial detentions and impunity (Kirchgaessner 2022).

The Mexican government denied that they used the spyware to target journalists and human rights defenders. Citizen Lab, however, stated that the use of this spyware by the government showed "flaw[ed] public accountability and transparency" (Kirchgaessner 2022). Pegasus was also found on the smartphones of people in the immediate vicinity of the then opposition political leader and current president Andrés Manuel López Obrador (Schächtele et al. 2022).

Case study: Harassment of human rights activists

Activists that document police violence and represent the victims of abuses that took place after a national strike and social protests have been subject to surveillance by the Colombian government. These included human rights and social justice organisations (ABC Colombia et al. 2020).

Two people working with a local CSO, Temblores ONG, decided to flee the country after receiving credible evidence that they were under surveillance (CIVICUS 2022). The human rights coalition Colombia-Europe-United States Coordination (CCEEUU) has also been subjected to surveillance. They claim a drone was flown around their office in Bogotá in November 2021, and an unauthorised phone was discovered in the car of one of their members (ABC Colombia et al. 2020). Asociación para la Investigación y la Acción Social has documented evidence that the national police have been using electronic surveillance against them, which may be the cause of the incidents of harassment that human rights defenders who work with them have experienced (ABC Colombia et al. 2020). In this case, the surveillance of these activists has led to real-life physical confrontations and harassment.

Case study: Deployment of spyware leading to the arrest of activists

The use of remote spyware against activists was a feature of the conflict in Syria (Hardy and Marquis-Bore 2012). This included a phishing campaign targeting a high-profile Syrian opposition figure and malware targeting activists by claiming to be documents regarding the foundation of a Syrian revolution leadership council, using software called Dark Comet RAT (Hardy and Marquis-Bore 2012).

Dark Comet RAT is software that steals passwords and contains a feature that helps it avoid detection by antivirus products (McMillan 2012). It can also record video and audio from a computer once it is installed (McMillan 2012). The activists believe that the Dark Comet malware led to many activists being arrested in Syria (McMillan 2012).

Development projects and surveillance malware

Humanitarian and development projects are at high risk of incidents such as security breaches of platforms and networks, as well as the exploitation of their systems against responders and

beneficiaries (Campo, Rymond and Scarnecchia 2017). Humanitarian organisations collect personal data on vulnerable populations on a mass scale to conduct their operations. For example, those working with refugees may be at risk from cyberattacks using spyware from militant groups, which was the risk noted by the humanitarian workers who were working with Syrian refugees that had fled ISIS (Bharania and Maitland 2017).

Another example or risks faced was a large data breach in 2022, when a group of unknown hackers hacked the systems of the International Committee of the Red Cross and accessed data on vulnerable populations across the world (Chen 2022). The individuals who had their data collected were particularly exposed as many had been separated from their families due to armed conflict, disasters and migration, and their names, locations and contact information were stolen (RSIS Commentary 2022).

Furthermore, some governments are implementing legislation to further facilitate, rather than regulate, the surveillance (which can include spyware) of development and humanitarian CSOs. For example, legislation in Russia in 2005 demanded re-registration procedures that affected 450,000 Russian CSOs operating in Russia (Hayes no date). This legislation created unprecedented control over independent CSOs and created a complicated registration procedure, as well as subjecting CSOs to inspections and audits at any time and without limitation (Hayes no date). Such abilities have given the Russian state increasing levels of power to conduct surveillance of the activities of these organisations through their extensive audits and inspections. And, while spyware has not necessarily been deployed in this instance, the legislative change could allow for more surveillance tools (such as spyware) to be used against Russian CSOs in the future.

In Colombia, an inspection by Grupo de Acción Financiera de Sudamérica (GAFISUD) found the country non-compliant with FATF Special Recommendation 8[2]. As a result, they recommended that the government review the sector to assess its vulnerability to terrorist financing and introduce a regulatory framework for CSOs (Hayes no date: 33). This included increased monitoring of CSOs.

However, Colombia is one of the most dangerous countries in the world to be an activist, and the recommendations to increase monitoring of CSOs have been criticised for not acknowledging this context (Hayes no date: 33). Indeed, on several occasions, the Inter-American Commission of Human Rights has raised its concern about threats against members of CSOs and the illegal surveillance of them (Hayes no date: 33). This type of legislation on the monitoring of CSOs could be used in the future to justify the use of spyware on activists and staff of CSOs and hindering the implementation of their project activities.

As such, the previous special rapporteur published a report on how international standards such as FATF have played a role in closing civic space, stating that FATF has lent "a veneer of legitimacy to states that, without due respect for their international human rights obligations, turned soft law to hard law by implementing the provisions of Recommendation 8 through wholesale measures that strictly regulate civil society, in violation of the

[2] Under the FATF Recommendation 8, governments should "review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism e.g. non-profit organisations" (FATF 2012-2022: 13)

principles of proportionality and necessity" (Human Rights Council 2019a).

Risk mitigation of surveillance malware

The role of civil society

CSOs have been collaborating and working with investigative journalists and cyber security professionals to investigate technology companies developing surveillance software and their work with governments, as well as advocating for greater transparency and integrity in the sector. These collaborations go beyond conventional circles and are fostering closer relations with the tech and cyber security industry.

For example, the human rights CSO Front Line Defenders collaborated with over 80 journalists in the investigation into the Pegasus scandal (Lee 2023). To uncover the scandal, they partnered with media agencies Le Monde, The Washington Post, Süddeutsche Zeitung and the Guardian (Lee 2023). This collaboration enabled a level of protection for the organisation, and they worked with Amnesty International to set up a secure encrypted system to communicate with the journalists to avoid being detected by the technology they were working to expose (Lee 2023).

Amnesty Tech is another global collective of advocates, hackers, researchers and technologists. They work with activists and other CSOs to build technological capacity to defend themselves against spyware and advocate against the risks posed by the surveillance industry (Amnesty Tech no date). Their Security Lab also leads technical investigations into cyberattacks against civil society and supports those who face attacks (Amnesty Tech no date).

Finally, the Citizen Lab conducts academic research into digital threats facing civil society and carries out high-level policy engagement. They also jointly investigated the NSO Group's Pegasus spyware being used on Palestinian human rights defenders. The Citizen Lab performed forensic analysis on the logs of devices to test whether they had been infected by Pegasus spyware (Citizen Lab 2021). They conduct targeted advocacy on the transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities (Citizen Lab no date).

Strengthening export controls

While some exporting states have adopted regulatory safeguards on surveillance software, these are often inconsistent, not keeping up to date with innovations in the technology and are often judged by experts to have not gone far enough. (Aho and Duffield 2020; Bromley 2020; D'Alessandra and Gildea 2022; Front Line Defenders 2021).

Indeed, even since scandals such as Cambridge Analytica's use of social media data to influence the US 2016 election, the US has failed to adopt any substantial data privacy laws at the federal level (Aho and Duffield 2020). Researchers point to the lobbying power of the tech industry and the profits of surveillance-centred business models that are provided to other industries as to reasons why it is difficult to regulate these markets (Aho and Duffield 2020).

In the EU, the dual-use functionality of surveillance software (that it can be used against criminals and civilians) has led to the EU passing the dual-use

regulation, which mandates certain transparency requirements and for manufacturers to assess risks to human rights (Schächtele et al. 2022). It also stipulates that the EU Commission maintains a checklist of specific technologies and destination countries for which exports much be approved in advance (Schächtele et al. 2022).

Nonetheless, many critics state that more binding controls of exports and comprehensive duty of care from European companies must be enacted, as many EU companies continue to sell their products to authoritarian regimes (Schächtele et al. 2022). Furthermore, there is currently no dedicated set of international rules that stop domestic companies from selling surveillance technologies to authoritarian regimes (D'Alessandra and Gildea 2022). To resolve this, some experts are calling for a comprehensive international agreement to be put into place on the export of dual-use surveillance technologies (D'Alessandra and Gildea 2022).

In light of the current regulatory limitations, some observers are calling for political decision makers to ban the export of surveillance products to other countries completely, other than for specific individual case authorisations (Schächtele et al. 2022).

Others, including the CSO Access Now and the UN special rapporteur on freedom of opinion and expression, David Kaye, call for an immediate global moratorium on the export, sale, transfer and use of surveillance technology until an adequate human rights regulatory framework is in place (Access Now 2022b; UN 2019). The report on the matter by Kaye emphasises that:

> "Surveillance tools can interfere with human rights, from the right to privacy and freedom of expression to rights of association and assembly, religious belief, non-discrimination, and public participation. And yet they are not subject to any effective global or national control" (UN 2019).

The UN Human Rights Council (2019) has also put forward recommendations to strengthen national legislation to regulate the export of surveillance products. It has called for the states that export surveillance technologies to ensure that public input is included in the formation of policies, and multi-stakeholder consultations be conducted when they are processing applications for export licences (Human Rights Council 2019b).

The council also recommends that exporting states join the Wassenaar Arrangement to mitigate the risks posed by spyware (Human Rights Council 2019). In this context, the Wassenaar Arrangement on the Export Controls for Conventional Arms and Dual-Use Goods and Technologies (1995) requires participating states to (Wassenaar Arrangement Secretariat 2019: 5):

- regularly meet to ensure the transfer of dual-use technologies are carried out responsibly and in furtherance of international and regional peace and security
- to share information that will enhance transparency on sensitive dual-use technologies and develop common understandings of the risks associated with these items
- to notify transfers and denials of dual-use technologies to other states
- to work on guidelines and procedures on dual-use technologies with continual review

The US President Joe Biden called for further export controls on dual-use technologies at the 2021 Summit for Democracy. The US, Australia, Denmark and Norway announced the Export Controls and Human Rights Initiative to help stem the tide of authoritarian misuse of technology

(White House 2021). The initiative plans to develop a voluntary written code of conduct to: guide the application of human rights criteria to export licensing policy and practice; build policy alignment with partners that leads to common action; and bring together policymakers, technical experts and human rights practitioners to manage emerging technologies (White House 2021). Critics note, however, that the proposals are tentative and only create a voluntary conduct to guide states in creating their own export licensing rules (D'Alessandra and Gildea 2022).

Increasing regulation and oversight of the use of surveillance software

Experts recommend that, in addition to export controls, a set of "cyber norms" should also be defined in the industry to prevent corruption and misuse (Alam and Chantzos 2016). These should be generally accepted principles of cyber behaviours that develop from legally binding norms or policy agreements at the domestic and international levels (Alam and Chantzos 2016).

Some observers have criticised the current regulations on the use of surveillance software in many countries, arguing that the levels of governance and safeguards are not advancing as fast as the technology. For example, despite the EU's General Data Protection Regulation (GDPR) being one of the most comprehensive laws for privacy and security, this was passed in 2014 when surveillance technologies were not as advanced as they are today (Miyamoto 2020: 57). Additionally, the GDPR rules do not apply to a government body or law enforcement agency if they are processing data for preventing threats to public safety (Compliance Junction 2019). This reasoning could in theory then be applied to justify protest surveillance, for example.

Alam and Chantzos (2016) argue that a collaboration between the cyber security industry and policymakers on the development of national and regional policies for the surveillance industry would ensure their relevance and practical implementation (Alam and Chantzos 2016). They note that policymakers often lack the technical understanding of new technologies, so this collaboration, alongside capacity building and training of officials will ensure more robust oversight and regulation of the industry (Alam and Chantzos 2016).

The report by the special rapporteur on the promotion and protection of the right to freedom of opinion and expression recommends that states impose a legal framework for the regulation, accountability and transparency of the use of surveillance technology (Human Rights Council 2019b). This includes (among others) that:

> "(a) States that purchase or use surveillance technologies ('purchasing States') should ensure that domestic laws permit their use only in accordance with the human rights standards of legality, necessity, and legitimacy of objectives, and establish legal mechanisms of redress consistent with their obligation to provide victims of surveillance-related abuses with an effective remedy.
>
> (b) Purchasing States should also establish mechanisms that ensure public or community approval, oversight and control of the purchase of surveillance technologies" (Human Rights Council 2019b: 20).

The report goes on to advise that states should "conduct independent, impartial and transparent investigations in cases of unlawful targeted surveillance against defenders working on

corruption" alongside the comprehensive measures to "prevent further violations linked to the sale, export and use of spyware technology" (Human Rights Council 2019b: 21).

Global Justice Clinic (2019) argues that states using the technology should always demonstrate the direct and immediate connection of the threat to justify any use of spyware (Global Justice Clinic 2019). They further recommend states to do the following to regulate technology companies developing surveillance software registered in their country (Global Justice Clinic 2019: 3):

- ensure there is an adequate legal framework for authorising any such targeting, which is subject to independent judicial review
- enact and enforce export control laws to prevent the sale of malicious software to governments that lack such minimal legal protections in their domestic laws
- undertake robust due diligence to ensure that government purchasers of software have those basic legal protections in place, that will afford individuals with procedural protections against wrongful targeting

Promoting integrity in technology companies that develop surveillance software

Instilling integrity within the surveillance industry is an important step to ensure that its technology is not abused for corrupt ends. Technological integrity includes principles that promote privacy measures and reject hidden functionalities or back-door channels in products that would weaken basic security technologies such as encryption (Alam and Chantzos 2016).

To ensure this, some researchers argue that companies should build communication technology that is fully encrypted, even if law enforcement agencies insist that they need to have access to communication for criminal investigations (Alam and Chantzos 2016: 204). The ability to conduct surveillance in itself opens more opportunities for criminals to take advantage (through security gaps that enable the surveillance).

Therefore, Alam and Chantzos argue that full encryption is necessary from the companies' side (Alam and Chantzos 2016: 204). They state that even in cases of "exceptional access" by governments to gain access to systems and data, companies should reject these requests to ensure the same loopholes cannot be exploited by criminals (Alam and Chantzos: 214). However, this would mean enforcement agencies would not be able to access communications if there is a genuine security threat.

Alarcón (2022) recommends that companies take a more human-centred approach in the design of their products and commit to transparency, accountability and respect for human rights and due diligence in their processes (Alarcón 2022). They should also provide remedies for the victims affected by their products (Alarcón 2022).

The report by the special rapporteur on the promotion and protection of the right to freedom of opinion and expression (2019) echoes the above recommendations from the literature and proposes the following principles for technology companies developing surveillance software:

(a) "Private surveillance companies should publicly affirm their responsibility to respect freedom of expression, privacy and related human rights, and integrate human rights due diligence processes from the earliest stages of product development and throughout their operations.

These processes should establish human rights by design, regular consultations with civil society (particularly groups at risk of surveillance), and robust transparency reporting on business activities that have an impact on human rights"

(b) And "companies should also put in place robust safeguards to ensure that any use of their products or services is compliant with human rights standards. These safeguards include contractual clauses that prohibit the customization, targeting, servicing or other use that violates international human rights law, technical design features to flag, prevent or mitigate misuse, and human rights audits and verification processes" (Human Rights Council 2019b).

The role of international donors

Finally, given the increased risk from spyware deployed by governments, the development and aid sectors need to prioritise cyber security throughout the development and implementation of their projects. The increased demand for data-driven approaches by international donors has led to vulnerable populations' personal data being collected by CSOs. Despite this, data protection is still largely under-funded (Chen 2022). International donors therefore have a responsibility to ensure that all funded projects build in a cyber security component to their programmes and provide adequate funding for these measures.

Donor governments can also support the above-mentioned policy initiatives in multilateral engagements. Promoting integrity in the sector and the standards held by the Wassenaar Arrangement, as well as the proposals put forward by CSOs, is important to ensure international standards on the industry are created and sustained. They can support initiatives such as calls for the adoption of a Digital Geneva Convention where governments would adopt and implement norms that have been developed to protect civilians (and by extension, civil society) on the internet (World Economic Forum 2017).

Other actions to mitigate the risks of spyware that researchers have put forward include the establishment of an independent ombuds office to report on critical data breaches in the development and humanitarian sector, as one does not currently exist (Chen 2022; Campo, Raymond and Scarnecchia 2017).

On the level of project implementation, project managers and other staff responsible for the implementation of development and humanitarian projects should be trained on how to protect themselves and their projects from cyber attacks and digital surveillance (Moßbrucker 2020). Suggestions put forward in the literature involve risk assessments and threat modelling in project inception, using protected communication mediums, creating a secure independent server for the organisation and protecting staff social media accounts with two-step authentication (Moßbrucker 2020). Nevertheless, these safeguards will only protect from smaller groups of hackers and might not protect CSOs from nation state actors conducting surveillance.

References

Aarvik P. 2022. Biometric data: Putting people at risk in the name of anti-corruption. U4 Anti-Corruption Resource Centre.

ABC Colombia et al. 2020. Alleged illegal espionage against lawyers from the Inter-church Commission of Justice and Peace (CIJP), José Alvear Restrepo Collective (CCAJAR), and other human rights defenders.

Access Now. 2022a. Navigating the surveillance technology ecosystem: A human rights due diligence guide for investors.

Access Now. 2022b. The Geneva Declaration on Targeted Surveillance and Human Rights.

Adam I. and Fazekas M. 2021. Are emerging technologies helping win the fight against corruption? A review of the state of evidence.

Aho B. and Duffield R. 2020. Beyond surveillance capitalism: Privacy, regulation, and big data in Europe and China. Economy and Society.

Alam S. and Chantzos I. 2016. Technological integrity and the role of emerging cyber norms. Chapter 10. International Cyber Norms: Legal, Policy and Industry Perspectives. NATO CCD COE Publications.

Alarcón A. 2022. What will it take for mass surveillance tech companies to respond on human rights? Access Now.

American Civil Liberties Union (ACLU). 2018. Stingray tracking devices: Who's got them?

Amnesty Tech. No date. Amnesty Tech.

Benjakob O., Breiner J., Scharft A. 2023. Israeli firm suspected of illegally selling classified spytech. Haaretz.

Bharania R. and Maitland C. 2017. Balancing security and other requirements in hastily formed networks: The case of the Syrian refugee response. SSRN.

Big Brother Watch Team. 2022. The Guardian – Chinese state-owned surveillance company launches sinister ethnicity recognition tech while facing UK ban.

Bromley M. 2020. A search for common ground: Export controls on surveillance technology and the role of the EU. About: Intel.

Campo S., Rymond N. and Scarnecchia D. 2017. Humanitarian data breaches: The real scandal is our collective inaction. The New Humanitarian.

Chen C. 2022. Cybersecurity in the humanitarian sector: New challenges and solutions. RSIS Commentary.

CIVICUS 2022. Colombia: Surveillance of civil society and detention of protest leaders.

CIVICUS. 2022. Palestinian CSOs branded "terrorist organisations" and surveilled by Pegasus spyware.

Citizen Lab. 2021. Devices of Palestinian human rights defenders hacked with NSO Group's Pegasus spyware.

Citizen Lab. No date. Transparency and accountability.

CIVICUS Monitor. 2020. Civic space on a downward spiral. Findings 2020.

Compliance Junction. 2019. Who is exempt from GDPR requirements?

Corera G. Pegasus scandal: Are we all becoming unknowing spies? BBC.

D'Alessandra and Gildea. 2022. We need international agreement on how to handle these dangerous technologies. Slate.

Edward-Gill J., Köbis N. C. and Starke C. 2022. The corruption risks of artificial intelligence. Transparency International.

Ersan. 2018. The human rights act and the electronic surveillance in Indonesia corruption eradication.

European Union (EU). No date. Exporting dual-use items.

Financial Action Task Force (FATF). 2012-2022. International standards on combating money laundering and the financing of terrorism and proliferation. The FATF Recommendations.

Fortinet. No date. What is a Trojan horse virus?

Front Line Defenders. 2021. OPT/Israel: Six Palestinian human rights defenders hacked with NSO Group's Pegasus spyware.

Global Justice Clinic. 2019. Attempted digital surveillance as a completed human rights violation: Why targeting human rights defenders infringes on rights. NYU School of Law.

Global NPO Coalition on FATF. Issues: On the obstructions faced by civil society organizations of this context.

Hardy S. and Marquis-Boire M. 2012. Syrian activists targeted with BlackShades spy software. The Citizen Lab. University of Toronto.

Harris E. No date. Technological characteristics and governance prospects. American Academy of Arts and Sciences.

Hayes B. No date. Legalising surveillance, regulating civil society. Transnational Institute/Statewatch.

Hern A. 2015. Hacking Team hacked: Firm sold spying tools to repressive regimes, documents claim. The Guardian.

Human Rights Council. 2019a. Impact of measures to address terrorism and violent extremism on civic space and the rights of civil society actors and human rights defenders. United Nations Digital Library.

Human Rights Council. 2019b. Surveillance and human rights report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression. United Nations General Assembly.

Kirabo J. 2021. Pegasus: Ugandan journalists targeted in spying scandal. Nile Post.

Kirchgaessner S. 2022. Mexico: Reporters and activists hacked with NSO spyware despite assurances. The Guardian.

Kirchgaessner S. and Taylor D. 2022. Nephew of jailed Hotel Rwanda dissident hacked by NSO spyware. The Guardian.

Knight B. 2022. Germany: Police surveillance software a legal headache. DW.

Lee C. 2023. 'Collaboration is protection': Journalists talk about investigating Pegasus spyware. PBS.

Marczak B. et al. 2014. Mapping Hacking Team's "untraceable" spyware. Citizen Lab.

McMillan. 2012. How the boy next door accidentally built a Syrian spy tool. Wired.

MENA Rights Group. 2020. NGOs: States use of digital surveillance technologies to fight pandemic must respect human rights.

Miyamoto I. 2020. Surveillance technology challenges political culture of democratic states.

Moßbrucker 2020. Threat modelling guide. How to identify digital risks in international development projects. Deutsche Welle. Bonn.

O'Neill P. H. 2019. The fall and rise of a spyware empire. MIT Technology Review.

Ozer N. 2016. Police use of social media surveillance software is escalating, and activists are in the digital crosshairs. ACLU.

Privacy International. 2016. The global surveillance industry. A report by Privacy International.

Privacy International. 2018. The global surveillance industry. Explainer.

Privacy International. No date a. Protest surveillance.

Privacy International. No date b. What governments do.

Richards N. 2013. The dangers of surveillance. Harvard Law Review. Vol 126:1934.

Schächtele et al. 2022. Digitalisation and civic space: Chances and challenges. Brot für die Welt. Analysis No 105.

Surveillance Self-Defence (SSD). No date. Malware. Glossary.

Tactical Tech. No date. Shrinking civil space: A digital perspective.

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). No date. Recast dual-use regulation - EU introduces new export controls on spyware.

Transparency International. No date. What is corruption?

United Nations (UN). 2019. UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools. Geneva.

Wassenaar Arrangement Secretariat. 2019. Wassenaar arrangement on export controls for conventional arms and dual-use goods and technologies. Public Documents Volume 1.

White House. 2021. Fact sheet: Export controls and human rights initiative launched at the summit for democracy. Briefing Room Statements and Releases.

World Economic Forum. 2017. Why we urgently need a Digital Geneva Convention. International Security.

Xu Xu. 2020. To Repress or to Co-opt? Authoritarian Control in the Age of Digital Surveillance. American Journal of Political Science. Volume 65, Issue 2 p. 309-325

Zetter K. 2020. How cops can secretly track your phone. The Intercept.

Zuboff S. 2015. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. Journal of Information Technology (2015) 30, 75–89.

DISCLAIMER
All views in this text are the author(s)' and may differ from the U4 partner agencies' policies.

PARTNER AGENCIES
GIZ/BMZ (Germany), Global Affairs Canada, Ministry for Foreign Affairs of Finland, Danida (Denmark), Sida (Sweden), SDC (Switzerland), Norad (Norway), UK Aid/FCDO.

ABOUT U4
The U4 anti-corruption helpdesk is a free research service exclusively for staff from U4 partner agencies. This service is a collaboration between U4 and Transparency International (TI) in Berlin, Germany. Researchers at TI run the helpdesk.

The U4 Anti-Corruption Resource Centre shares research and evidence to help international development actors get sustainable results. The centre is part of Chr. Michelsen Institute (CMI) in Bergen, Norway – a research institute on global development and human rights.

www.U4.no
U4@cmi.no

KEYWORDS
Surveillance – activists – civic space– accountability