



DCAF Geneva Centre
for Security Sector
Governance



**PRIVACY
INTERNATIONAL**

UNDERSTANDING PRIVATE SURVEILLANCE PROVIDERS AND TECHNOLOGIES

**WITHIN THE WIDER FRAMEWORK
OF PRIVATE SECURITY GOVERNANCE**

Acknowledgements

This policy paper was developed by DCAF – Geneva Centre for Security Sector Governance in cooperation with Privacy International. An invitation-only roundtable was organized in December 2022 in Geneva, bringing together private security regulators and experts, and its key findings were included in the document.

We would like to thank the Peace and Human Rights Division and the Export Controls and Private Security Services Section of the Swiss Federal Department of Foreign Affairs (FDFA) as well as the United Kingdom's Foreign Commonwealth and Development Office (FCDO) for their generous support. For developing the policy paper, we thank Iliia Siatitsa, Gabrielle Priklopilova, Jean-Michel Rousseau, Edin Omanovic, Rebecca Stephan and Christopher Crosby. For valuable feedback and contributions, we thank Megan Bastick, Vincent Bernard, Orlando Bianchetti, Ferdinand Chukwudi Esiegwu, Fernando Frenkle, Martina Gasser, Sorcha MacLeod, Chinwike Okereke, Antoine Perret, Manuel Rodriguez, and Paulo Cesar Zevallos Rivalola.

DCAF

The Geneva Centre for Security Sector Governance (DCAF) is an organization dedicated to improving the security of people and the states they live in within a framework of democratic governance, rule of law and human rights. DCAF assists partner states, and international actors supporting these states, to improve the governance of their security sector through inclusive and participatory reforms based on international norms and good practices. DCAF provides policy advice, promotes norms and good practices, and supports capacity building of governmental and non-governmental security sector stakeholders, as well as of intergovernmental organizations, to support security sector reform processes.

Privacy International

Privacy International (PI) is a London-based non-profit, non-governmental organisation (charity number: 1147471) that challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy. Within its range of activities, PI investigates how people's personal data is generated and exploited and, how it can be protected through legal frameworks and technology solutions. It further advocates and litigates globally to put pressure on companies and governments to change.

Understanding Private Surveillance Providers and Technologies within the Wider Framework of Private Security Governance

ABSTRACT

This policy paper seeks to determine the potential for the existing international private military and security companies (PMSC) regulatory framework to support more effective regulation of private surveillance services. In order to achieve this, and given that this paper addresses an issue that is at the intersection of the two domains, it seeks to establish a common language and terminology between security sector governance (SSG) and surveillance practitioners. In section I, the paper offers an introduction to the different private surveillance technologies and services. In understanding the scope of surveillance capabilities, it becomes possible to be able to evaluate to what extent they could be considered as private security services. This also becomes true when addressing the companies offering such services and technologies as private security providers. Section II provides some examples of how surveillance impacts the right to privacy and other human rights. It highlights how infringements of the right to privacy by private surveillance providers and technologies result in chains of cause and effect on other rights (such as the right to life). Section III observes and evaluates how existing international norms and good practices for private security regulation (namely, the Montreux Document, the International Code of Conduct and the UN Guiding Principles on Business and Human Rights) can serve as a basis for strengthening the regulation of some private surveillance providers and technologies. It further offers specific recommendations on next steps and actions that need to be taken to ensure that private surveillance services are appropriately and effectively covered and overseen by the PMSC regulatory framework.



INTRODUCTION

Provision of surveillance equipment and services to government authorities and private clients has risen dramatically in recent years.¹ When law enforcement and intelligence agencies are adequately regulated and overseen, these capacities have the potential to assist law enforcement and border management, as well as counterterrorism operations. However, surveillance services and technologies are also under intense scrutiny for the danger they can represent for democracy, human rights and good security-sector governance. The Pegasus revelations, amongst others,

have highlighted how such technology could be used to target human rights defenders, including journalists.² In addition to targeted spyware, a broad range of private security companies are providing surveillance technologies and services, including surveillance-for-hire services, that are being marketed and sold to government agencies and private clients around the world. This poses pressing questions regarding the wider regulatory, monitoring and accountability frameworks for these services.

Defining Surveillance

There is no globally-agreed definition of the term 'surveillance'. The US Department of Defence classifies it as 'the systematic observation of aerospace, cyberspace, surface, or subsurface areas, places, persons, or things by visual, aural, electronic, photographic, or other means'.³ Some jurisdictions define the term within legislative texts; for example, in the UK, surveillance is defined within the Covert Surveillance and Property Interference Revised Code of Practice as including the 'monitoring, observing or listening to persons, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained'.⁴ Yet other laws in the UK refrain from providing a definition.

For the purposes of this paper, the term 'surveillance' is used to refer to the 'scrutiny of individuals, groups and contexts using technical means to extract or create information'.⁵ This includes the scrutiny of personal data, as well as data that is not personal or has been anonymised (for example, mobile phone location data that a company claims has been anonymised).

- 1 UNHRC, 'Report of the Office of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age' (4 August 2022), UN Doc A/HRC/51/17, para 42. All references hereinafter accessed on 26 June 2023; Access Now, 'Defending peaceful assembly and association in the digital age: takedowns, shutdowns, and surveillance', July 2020, www.accessnow.org/wp-content/uploads/2020/07/Defending-Peaceful-Assembly-Association-Digital-Age.pdf. See also Sharon Weinberger, 'Private Surveillance is a Lethal Weapon Anybody Can Buy. Is it too late to rein it in?' New York Times (19 July 2019), www.nytimes.com/2019/07/19/opinion/private-surveillance-industry.html.
- 2 See below, Examples 3 and 7.
- 3 Department of Defence (DOD) *Dictionary of Military and Associated Terms* (November 2021), www.supremecourt.gov/opinions/URLs_Cited/OT2021/21A477/21A477-1.pdf
- 4 UK Home Office, *Covert Surveillance and Property Interference*, Revised Code of Practice, 2018, assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf
- 5 Gary Marx, *Routledge Handbook of Surveillance Studies* (Abingdon, Routledge, 2012).

Increased awareness of the impact of private surveillance services and technologies on democracy, human rights and good security sector governance has led to increased calls to strengthen its regulation. In one pertinent example, the UN Special Rapporteur on freedom of expression concluded in their private surveillance industry report that there was a need for tighter regulation of surveillance exports and the restrictions on their use.⁶ Moreover, the report calls 'for an immediate moratorium on the global sale and transfer of the tools of the private surveillance industry until rigorous human rights safeguards are put in place to regulate such practices and guarantee that governments and non-state actors use the tools in legitimate ways'.⁷

In this context, it is of relevance to understand the international norms and good practices that have already been developed since the 2000s to address the overall field of PMSC. Despite the fact that private surveillance providers that offer surveillance technologies and surveillance services are often not regulated as PMSC, they do fall under the internationally established sector definition of 'private business entities that provide military and/or security services, irrespective of how they describe themselves'.⁸ These norms and good practices thus constitute a valuable base upon which to strengthen the regulation of this set of services at international and national levels.⁹

Given the aforementioned considerations, there are open questions as to what kinds of surveillance services and technologies fall within such definitions, as well as whether such norms and best practices can effectively provide safeguards against human rights abuses.¹⁰ This paper seeks to determine the potential for the existing international PMSC regulatory framework to support more effective regulation of private security companies that are providing surveillance services.

A common language between security sector governance (SSG) and surveillance practitioners needs to be found, as this subject touches upon these two domains. For the purpose of this paper, the focus is on companies that provide surveillance services. However, this does not include the entire spectrum of companies developing surveillance technologies. It is clear that understanding how such technologies work determines how corresponding services affect human rights. Thus, this paper first examines surveillance technologies and services as regards their link to security (section I), and then it analyses their impact on human rights (section II). The paper concludes in section III by formulating recommendations on how to apply and better implement the PMSC regulatory framework in order to mitigate the negative impact on democracy, human rights and good security-sector governance of private security companies' provision of surveillance services.

6 UNHRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on surveillance and human rights' (28 May 2019), UN Doc A/HRC/41/35 (hereinafter Report of the Special Rapporteur, A/HRC/41/35), undocs.org/A/HRC/41/35.

7 Ibid para 2.

8 Montreux Document on Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security Companies During Armed Conflict, September 2008 (hereinafter Montreux Document).

9 As suggested by the UN Special Rapporteur on Freedom of Expression, 'the co-regulation of private security companies requires efforts to educate companies about human rights concerns and creates incentives for multi-stakeholder participation (certification based on civil society-inclusive audit and monitoring processes), which may transfer well to the private surveillance industry'. Report of the Special Rapporteur A/HRC/41/35, para 61.

10 For example, export controls regulation of dual-use goods, such as the Wassenaar Arrangement, includes certain surveillance technology (goods). The EU has also recently updated its Dual-Use Regulation (EU) 2021/821 to include a catch-all clause for cyber-surveillance items in Article 5. 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) [2021] OJ L206/1. However, services in connection with such items or surveillance services provided without an export of items are not covered. See paper by Heejin Kim, 'Global Export Controls of Cyber Surveillance Technology and the Disrupted Triangular Dialogue' (2021) 70(2) *International & Comparative Law Quarterly* 379.

PRIVATE SURVEILLANCE PROVIDERS, TECHNOLOGIES AND SERVICES

This section briefly presents examples of the different private surveillance providers, technologies and services – including communication operators – in order to provide an overview of the scope of surveillance capabilities that could be seen as part of services provided by private security providers. It is not meant to be exhaustive but rather to give a brief overview.

Private security companies providing surveillance services are ‘private business entities that provide military and/or security services, irrespective of how they describe themselves’.¹¹ Surveillance companies include all private companies that market hardware and software for the explicit purpose of conducting surveillance for law enforcement, for intelligence or for security purposes. Surveillance companies are often considered as being a part of the ‘cybersecurity’ industry, but there are important differences between them. The cybersecurity industry generally offers a

range of technologies and services, used to protect networks and devices from unauthorised intrusion, detecting such intrusions along with responding to and recovering from such attacks.¹² In such cases, it may be necessary to monitor networks or devices for these purposes. While surveillance companies may sell similar technologies and services to monitor networks or devices, they do so in order to obtain information on natural persons for the purpose of intelligence or law enforcement.

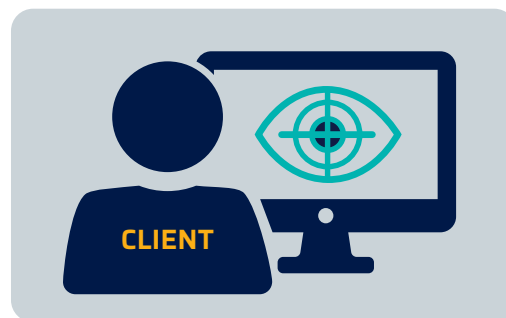
TECHNOLOGY OR TECHNOLOGY SERVICE PROVIDER?

Technology Service Provider



The technology service provider offers expertise and/or operates the technology.

Technology Provider



The company only provides hardware and/or software.

Technology Available to Private Security Companies Providing Surveillance Services

This paper focuses on the regulation of private security companies providing surveillance services. For the purposes of this policy paper, as defined just above, surveillance companies are understood as companies that market hardware and software for the explicit purpose of conducting surveillance for law enforcement, for intelligence or for security purposes. This does not include the entire spectrum of companies providing surveillance technologies. In practice, technology providers are difficult to differentiate from service providers. This is a result, among others, of some cases where technology developers offer services to support the use of their product. For the purpose of regulation and oversight, it is essential to understand the range of surveillance technologies available to private security companies providing surveillance.

¹¹ Montreux Document, above.

¹² UK, Department for International Trade, ‘Cyber Security Export Strategy’ (2018), assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/693989/CC5151_CC50118810124-1_Cyber_Security_Export_Strategy_Brochure_Web_Accessible.pdf.

By using information collected at trade shows and what is available publicly online, Privacy International (PI) identified some 528 surveillance companies already in 2016. These companies are overwhelmingly based in large arms-exporting countries.¹³ This suggests a link between the armament industry and the surveillance sector. Many of these companies' products and employees are recruited from intelligence and security

agencies in their country of origin: for example, former agents in intelligence agencies may go on to establish surveillance companies using their training and knowledge.¹⁴ Below, we review the different types of surveillance companies that may fall within the scope of the Montreux Document: a private actor that collects and/or processes surveillance data *for security and/or military purposes*.

'SURVEILLANCE-AS-A-SERVICE': RESEARCH, CONSULTATION AND/OR TRAINING

Companies that offer 'surveillance-as-a-service' deliver raw data or intelligence. They are sourced from a wide variety of sectors. The list includes large consultancies, private investigation, risk analysis, public relations and crisis management. In general, these companies provide services to both government and corporate customers. As such, they rely on a wide range of surveillance techniques, from open-source data scraping to hacking devices.

Some companies do not provide software or hardware themselves, but they do provide training in surveillance techniques or technical systems that can be used for surveillance (see Example 2). This branch of the industry has received significant exposure in recent years due to the use of such companies by political parties during elections (see Example 1).

Example 1 | Surveillance-as-a-Service - Cambridge Analytica

Reports have shown how data consultancy Cambridge Analytica used datasets derived from Facebook to profile and to target individual voters, with the aim of predicting and influencing their voting decisions in the US and the UK.¹⁵

Example 2 | Training - Civipol

Civipol was founded in 2001. It is part-owned by the French state and by large arms producers, including Thales, Airbus DS and Safran.¹⁶ It describes itself as the technical cooperation operator of the French Ministry of the Interior, and it offers audit, project management, training and consulting services in France and abroad. Training courses offered by Civipol, amongst its other services, include 'technological tracing/ identification of cell phone location', 'using digital data collected during searches' and general 'Investigation techniques'.¹⁷

¹³ PI, 'The Global Surveillance Industry' (2016), www.privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf.

¹⁴ Amos Barshad, 'Inside Israel's lucrative – and secretive – cybersurveillance industry' *Rest of World* (9 March 2021), restofworld.org/2021/inside-israels-lucrative-and-secretive-cybersurveillance-talent-pipeline/.

¹⁵ PI, 'Cambridge Analytica, GDPR – 1 year on – a lot of words and some action' (2019), privacyinternational.org/news-analysis/2857/cambridge-analytica-gdpr-1-year-lot-words-and-some-action

¹⁶ Civipol, 'The company', www.civipol.fr/en/civipol/company.

¹⁷ Civipol, 'Missions', www.civipol.fr/en/missions-et-projets/missions.

TECHNOLOGY DEVELOPERS AND MARKETERS

These companies sell a variety of technologies, and they market themselves as surveillance companies. In many circumstances, their technology is allegedly sold only to government end-users, because using it would be illegal under national laws for corporate or for non-governmental entities (see Example 3).

Example 3 | Technology Developers and Marketers – NSO Group

NSO Group is an Israeli surveillance company specialising in spyware. This spyware is used to take control of the functions of devices (such as the webcam) and to extract data. The company states that ‘NSO products are used exclusively by government intelligence and law enforcement agencies to fight crime and terror’.¹⁸ It is believed that the Group’s founders served in Unit 8200, the Signals Intelligence Unit of the Israeli Defence Force.¹⁹ In 2019, Moody’s reported that NSO Group had over 60 customers, in more than 35 countries, and over 600 employees.²⁰ The company’s technology has been repeatedly reported to have been used to target human rights defenders, journalists and others.²¹ See also further below ‘Example 7: The Pegasus Revelations’.

Dual-use companies, in the surveillance context, include companies that may sell technology that can be used for cybersecurity or intelligence, law enforcement or security purposes. Dual-use technology companies present a qualification challenge in determining whether a company provides security technologies or services in the context of surveillance. Such companies may sell technology that can be used to monitor networks to protect against intrusion or for quality of service. For example, a company might ensure that traffic flowing through a network is doing so efficiently. In short, although the technology would have been developed for the purpose of cybersecurity, it could in fact be used for surveillance (see Example 4).

Example 4 | Dual-Use Technology Companies – Sandvine

Based in Canada, Sandvine sells ‘Active Network Intelligence’ marketed to telecommunications operators. Its products rely on Deep Packet Inspection (DPI) technology, which is used to monitor internet traffic. Sandvine states that its customers can utilise monitoring in order to understand ‘contextual performance between subscribers, their devices, and the services they consume’ and, for example, to ‘ensure accurate charging’. However, DPI is also reported to be routinely used around the world for surveillance, censorship and behavioural targeting.²² In 2018, the Citizen Lab found that DPI boxes were being used to redirect hundreds of users in Turkey and Syria to nation-state spyware when those users attempted to download certain legitimate Microsoft Windows applications.²³ Similar DPI boxes were found in Egypt. These boxes had characteristics of the network injection in Syria and Egypt and matched Sandvine PacketLogic devices.²⁴

18 NSO Group, www.nsoagroup.com/about-us/.

19 Thomas Brewster, ‘Everything We Know About NSO Group: The Professional Spies Who Hacked iPhones With A Single Text’ *Forbes* (25 August 2016), www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/?sh=27baa4613997.

20 Moody’s, www.moody.com/research/Moodys-assigns-B2-CFR-to-NSO-Group-outlook-stable--PR_396559.

21 Citizen Lab, ‘NSO Group’, citizenlab.ca/tag/nso-group/.

22 EPIC, ‘Deep Packet Inspection and Privacy’ (2009), epic.org/privacy/dpi/#background.

23 Bill Marczak et al, ‘Sandvine’s Packet Logic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?’ *Citizen Lab* (9 March 2018), citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/.

24 Ibid.

TYPES OF SURVEILLANCE

COMMUNICATION

Intercepting signal traffic or its metadata

Internet Protocol Surveillance Systems | Explicitly designed to intercept internet traffic for law enforcement or intelligence purposes.

Lawful Interception Systems | Intercept the content of communications and metadata from telecommunications networks and provide them to a law enforcement agency for security purposes.

Device and system interference

IMSI Catchers | Ascertain unique characteristics of device such as the 'International Mobile Subscriber Identity (IMSI)' code, and in some cases intercept call or message content.

Spyware | Generally targets devices with malware – malicious software – can be used for remote monitoring in real time, by for example covertly eavesdropping on the microphone.

Mobile phone (and other devices) extraction tools | Digital forensics' tools which – when connected to a device – can download its content, including content the user believes has been deleted.

BIOMETRIC

Gathering data on the physiological and behavioural characteristics of individuals

Fingerprints, voice, face, retina, iris patterns, hand geometry, gait, or DNA profiles, etc.

COMMUNICATIONS OPERATORS

Telecommunication service providers manage landline, mobile (cell) or internet networks. They are generally public-facing and well-known national and international brands, such as AT&T or Deutsche Telekom. They are not traditionally seen as 'private security service providers'. However, such operators could be categorised as private security providers when they facilitate surveillance. In order to obtain operating licences, they need to conform to technical standards to ensure that state authorities can access data (see Example 5). In Europe, for example, the EU mandates that such operators must ensure government agencies can intercept data on their networks. Moreover, they can implement technical standards developed by the European Telecommunications Standards Institute (ETSI), as they facilitate 'lawful interception'. Operators in other jurisdictions, such as in post-Soviet countries or in North America, abide by different legal obligations and technical standards.²⁵

When these networks provide lawful interception capabilities to government agencies, they rely on technical infrastructure that is sold by a number of surveillance and telecommunications companies. For example, Ericsson and Cisco – two of the world's largest manufacturers of telecommunications equipment – either sell such 'lawful interception' systems to network operators directly or they design their equipment in such a way as to ensure lawful interception' functionality.²⁶

Example 5 | Communications Operators – Vodafone

Since 2013, Vodafone has reported annually on how the company and its subsidiaries comply with government surveillance demands in the 28 countries in which they operate.²⁷ While these annual reports seek to disclose how many times Vodafone has provided call content or call 'metadata' (the who, what, where and when of calls) to authorities, it is restricted from doing so in most countries. In regard to Egypt, for example, the 2019–20 report provides no statistics for how often Vodafone has complied with government requests for access to data. Vodafone states that the law in Egypt 'allows broad latitude to the armed forces and security agencies to obtain information pursuant to national security concerns, which are not defined', and that these authorities have 'broad latitude to intercept communications with or without an operator's control or oversight'.²⁸

25 PI, 'Lawful interception: the Russian approach' (2013), privacyinternational.org/blog/1296/lawful-interception-russian-approach.

26 Ericsson.com, Regulatory products, www.ericsson.com/en/portfolio/cloud-software--services/cloud-core/communication-services--udm/regulatory-products; Cisco, Lawful Intercept Overview, www.cisco.com/c/en/us/td/docs/routers/10000/10008/feature/guides/lawful_intercept/10Llavr.html.

27 Vodafone, 'Country by Country Disclosure of Law Enforcement Assistance Demands 2019–20', www.vodafone.com/sites/default/files/2021-02/Vodafone_LED_country_by_country_2019-20.pdf.

28 Ibid.

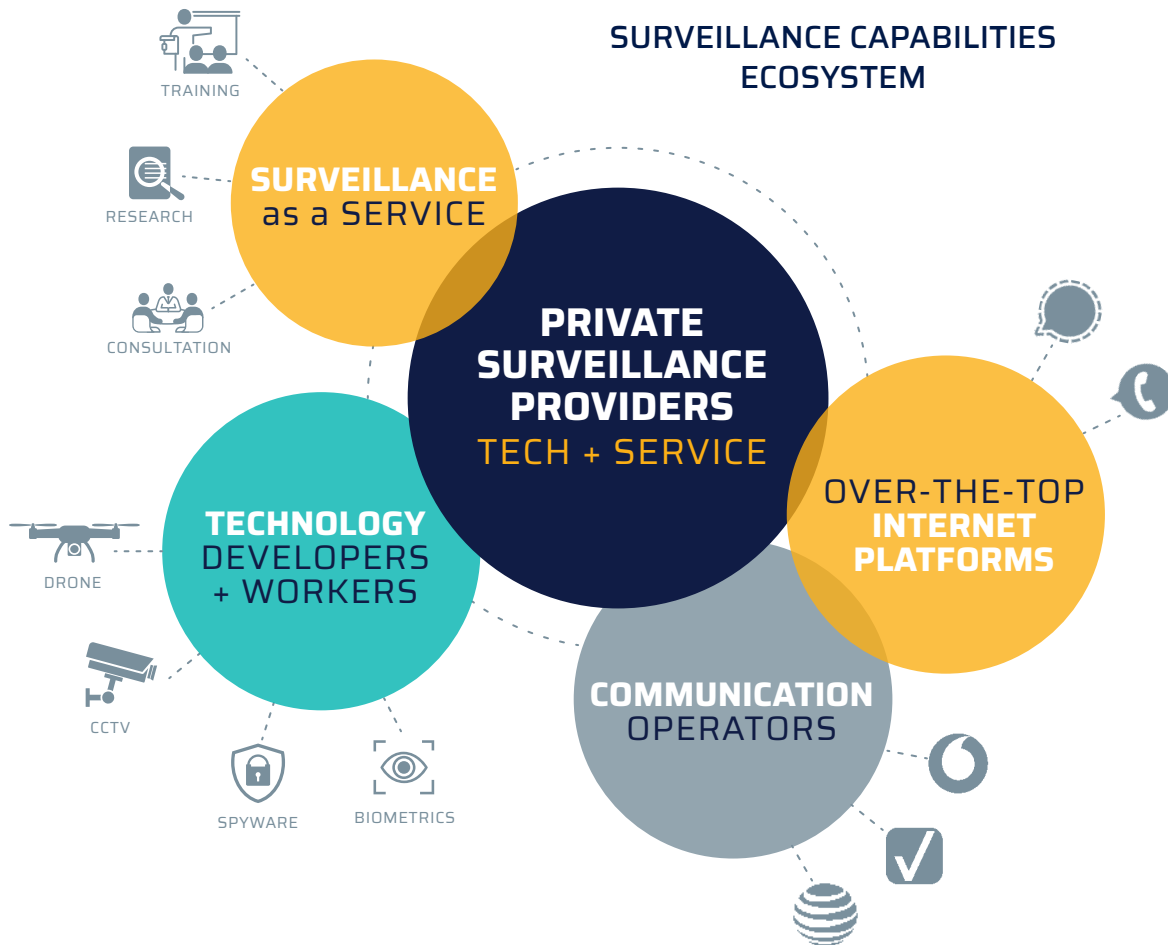
‘OVER-THE-TOP’ INTERNET PLATFORMS

The term ‘over-the-top’ implies that a content (or service) provider is going over the top of existing internet services. In other words, they are known as ‘over-the-top’ platforms because they rely on the technical telecommunications infrastructure provided by operators. This can include a wider range of companies, including apps available on mobile (cell) phones. Communications platforms and online services, such as WhatsApp, are not generally associated with private surveillance. However, they could potentially provide surveillance services. They could be able to grant access to data centres or decrypt and provide communications to third parties. The extent to which over-the-top providers collect and disclose user data varies widely between platforms (see Example 6). Generally, such providers have in practice not provided government access to data in many jurisdictions either because they are based abroad and unresponsive to government requests, or because – using the US as an

example case – the surveillance laws do not authorise such access.²⁹ In response, jurisdictions around the world are passing laws aimed at forcing such providers to give government access. This is completed either by allowing direct access to their data centres, or by forcing the providers to decrypt and hand over communications subject to a judicial order.³⁰

Example 6 | Over-the-Top Internet Platforms – Signal

Signal, a non-profit organisation using end-to-end encrypted technology, maintains that, even under a subpoena by US courts, it is capable of providing only basic information about when an account was created and last used, because it does not collect any message content or metadata.³¹



29 Justin (Gus) Hurwitz, ‘Encryption Congress Mod (Apple+CALEA)’ (2017) 30(2) *Harvard Journal of Law & Technology* 355, scholarship.law.upenn.edu/faculty_articles/270.

30 ‘Russia lifts ban on Telegram messaging app after failing to block it’ *Reuters* (18 June 2020), www.reuters.com/article/us-russia-telegram-ban-idUSKBN23P2FT; ‘Five Eyes’ security alliance calls for access to encrypted material’ *Reuters* (30 July 2019), www.reuters.com/article/us-security-fiveeyes-britain-idUSKCN1UP199

31 Signal, ‘Grand jury subpoena for Signal user data, Central District of California’ (27 April 2021), signal.org/bigbrother/central-california-grand-jury/

PRIVATE SURVEILLANCE AND HUMAN RIGHTS

This section provides some examples of how surveillance technology and services work and how they impact the right to privacy. It ends with showing how infringements of the right to privacy by private surveillance providers and technologies have ripple effects on other rights, such as the right to life.

Private surveillance for security and/or military purposes is conducted by a wide range of actors beyond the classical security sector, including private investigators, software developers and communication operators. Such technology has a significant impact on human rights. The private sector dominance of this technology raises concerns linked to state sovereignty and control, as well as questions of accountability and access to effective remedies for potential victims of human rights violations.³² This section starts off by looking at the right to privacy, highlighting its role in connection with the enjoyment of other human rights. Both the UN General Assembly and the UN Human Rights Council have reaffirmed that the right to privacy is one of the foundations of democratic societies; therefore, it plays an important role in the realisation of the rights to freedom of opinion and expression, as well as the freedoms of peaceful assembly and association.³³ Privacy is a right that also enables the enjoyment of other rights. In consequence, interference with privacy often opens the gate to the violation of the rest of human rights, including the right to life, freedom of peaceful assembly, fair trial and others.³⁴ Hence, the impact on other basic human rights will also be examined.

SURVEILLANCE AND THE RIGHT TO PRIVACY

Privacy may be understood as a space for individuals to have autonomous development, liberty and interaction. Additionally, it includes freedom from excessive unsolicited intervention by uninvited individuals or groups – including the state and private surveillance companies.³⁵ The right to privacy is enshrined in many international and regional human rights instruments, including in Article 17 of the International Covenant on Civil and Political Rights (ICCPR).³⁶ Article 17 of the ICCPR stipulates that, while privacy is not an absolute right, it must be protected against unlawful or arbitrary interference. Therefore, any interference with the right to privacy must be pursuant to a domestic legal basis that is foreseeable, accessible and provides for adequate legal safeguards against abuse.

Restrictions on the right to privacy must be aimed at protecting a legitimate aim, with due regard to the principles of necessity, proportionality and non-discrimination.³⁷ The UN Human Rights Committee – the monitoring mechanism of the ICCPR – determined that the right to privacy required robust and independent oversight systems to be put in place regarding surveillance, interception and hacking. Furthermore, authorities must ensure that the judiciary was involved in the authorisation of such measures in all cases.³⁸ In the event of infringements of the right to privacy, when found to be in violation of international human rights standards, states must provide for an effective remedy, including, where possible, retrospective notification that the subjects had been placed under surveillance.³⁹

32 Anne-Marie Buzatu, 'From Boots on The Ground to Bytes in Cyberspace: a Mapping Study on the Use of Information Communications Technologies (ICTs) in Security Services provided by Commercial Actors', ICT4Peace Foundation, 2022.

33 For example, The right to privacy in the digital age, UNGA Res 75/176, 16 December 2020; The right to privacy in the digital age, UNHRC Res 48/4, 7 October 2021, undocs.org/A/HRC/RES/48/4.

34 PI, 'Privacy Matters', privacyinternational.org/learning-resources/privacy-matters.

35 UNHRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (17 April 2013), UN Doc A/HRC/23/40, undocs.org/A/HRC/23/40.

36 See also Article 8, European Convention on Human Rights (ECHR); Article 11, American Convention on Human Rights (ACHR); Articles 16 and 21, Arab Charter on Human Rights; Article 16, Convention on the Rights of the Child (CRC) and others.

37 See references, PI's Guide to International Law and Surveillance, December 2021, privacyinternational.org/sites/default/files/2022-01/2021%20GILS%20version%203.0_0.pdf.

38 UN Human Rights Committee, Concluding Observations on the Sixth Periodic Report of Italy, UN Doc CCPR/C/ITA/CO/6, 28 March 2017, para 36 (hereinafter Concluding Observations on Italy).

39 Article 2(3) ICCPR; Article 13 ECHR. See also Concluding Observations on Italy, para 37.

Communications Surveillance

The UN General Assembly highlighted that

*the rapid pace of technological development enables individuals all over the world to use new information and communications technologies, and at the same time, it enhances the capacity of Governments, business enterprises and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights, in particular, the right to privacy [...]*⁴⁰

There are different ways and methods by which private companies can conduct surveillance on communication. Some companies that conduct communications surveillance rely on intercepting signal traffic or its metadata. For example, this may include the interception of calls, emails, VoIP messages or internet browsing history. These tools do not target devices, or ‘end-points’; instead, they target signals in transit. This category of surveillance includes, amongst others, the use of:

- ▶ **Lawful Interception Systems**, which intercept the content of communications and metadata from telecommunications networks to then provide them to law enforcement agencies for security purposes.⁴¹
- ▶ **Internet Protocol Surveillance Systems**, which are explicitly designed to intercept internet traffic for law enforcement or intelligence purposes, and which may rely on DPI techniques. These may be fitted inside telecommunications networks.⁴²

While the communications services described above target data traffic or metadata, other companies use mobile (cell) device interference that targets devices, known as ‘end-points’. For example:

- ▶ **IMSI Catchers**. These devices act as mobile (cell) phone towers so that mobile (cell) devices connect to them.⁴³ By doing so, IMSI Catchers are able to ascertain certain unique characteristics of the particular device, such as the International Mobile Subscriber Identity (IMSI) code, and, in some cases, intercept calls or message content.
- ▶ **Spyware**. Such tools generally target devices with malware – malicious software – which is developed with the intention of extracting data from a device or controlling its functions (eg, a microphone). Accordingly, such spyware allows a government agency intrusive access to the contents of a person’s device, including encrypted applications such as Signal, and this can be used for remote monitoring in real time. An example of this situation would be covertly eavesdropping on the microphone. While ‘hacking’ services are easily available online,⁴⁴ the advanced companies on the surveillance market rely on developing sophisticated code that can bypass the protections found on common devices. This would deter the majority of attacks (see Example 7).⁴⁵ Spyware and other hacking services can be used by government agencies as well as private companies.
- ▶ **Extraction**. This refers to digital forensics tools that, when connected to a device, can download its content. Thereafter, such tools can access large amounts of data contained within devices – including, often, content the user believes has been deleted.⁴⁶

40 The right to privacy in the digital age, UNGA Res 75/176, 16 December 2020, undocs.org/A/RES/75/176.

41 For example, Utimaco, ‘Lawful Interception of Telecommunication Services’, assets.documentcloud.org/documents/804664/1233_utimaco_product-description.pdf.

42 For example, ETI Group, Excellence through specialisation, assets.documentcloud.org/documents/711361/brochure539.pdf.

43 PI, ‘IMSI Catchers Explainer’ (2018), privacyinternational.org/explainer/2222/imsi-catchers.

44 James Coker, ‘High Demand for Hacker Services on Dark Web Forums’ *Infosecurity magazine* (2021), www.infosecurity-magazine.com/news/demand-hacker-services-dark-web/.

45 See, PI, ‘An Open Source Guide to Researching Surveillance Transfers’ (2018), privacyinternational.org/long-read/2225/open-source-guide-researching-surveillance-transfers.

46 PI, ‘A technical look at Phone Extraction’ (2019), privacyinternational.org/long-read/3256/technical-look-phone-extraction.

The different methods of communication surveillance described above explain how private security companies providing surveillance services can access the content of communications either while they are taking place or after the fact. Furthermore, they are able to access

the content of a communications device through diverse means and techniques. These technologies can overcome data protection mechanisms built into the devices, and they can access data the holders themselves do not know they have.

Example 7 | The Pegasus Revelations

Researchers, journalists, activists and others have uncovered significant evidence over the years of the use of NSO Group's surveillance technology to target individuals around the world in violation of their internationally-recognised human rights.⁴⁷ Amongst others, the Forbidden Stories consortium, a Paris-based journalism non-profit, and Amnesty International gained access to a list of more than 50,000 phone numbers of potential and actual surveillance targets.⁴⁸ Combined with forensic analysis of numerous infected phones, it was revealed that at least 189 journalists, 85 human rights defenders and over 600 politicians and government officials were affected as targets.⁴⁹

The Pegasus spyware can turn any smartphone into a 24-hour surveillance device. It requires zero clicks to infect a phone, and it can evade most forensic analysis while avoiding detection by firewalls and anti-virus software.⁵⁰ Once infected by Pegasus, virtually all data can be retrieved and stored, such as telecommunications, messages, photos and geographic location. Cameras and microphones can be activated remotely to conduct live surveillance of targets.

Such practices pose grave and unique threats to the privacy of millions of people. Given that many tools and services provided by private surveillance companies risk infringing on this space, their practices have a serious impact on the right to privacy. Any interference should comply with human rights standards. In addition, there is a gendered and intimate dimension to the threats to privacy, as electronic surveillance is widely used in stalking and domestic violence contexts of coercive control (eg, abusers installing covert cameras or GPS tracking devices).⁵¹

The UN General Assembly has condemned unlawful or arbitrary surveillance and interception of communications as 'highly intrusive acts' that interfere with fundamental human rights.⁵² States are primarily responsible for taking the necessary steps to adopt laws or other measures to give effect to the rights recognised in the ICCPR and other international instruments providing relevant obligations and standards.

47 Dana Priest and Elizabeth Dvoskin, 'Chief of WhatsApp, which sued NSO over alleged hacking of its product, disputes firm's denials on scope of involvement in spyware operations' *The Washington Post* (24 July 2021), www.washingtonpost.com/investigations/2021/07/24/whatsapp-pegasus-spyware/.

48 Forbidden stories, 'About the Pegasus Project', forbiddenstories.org/about-the-pegasus-project/.

49 UNHRC, 'Report of the Office of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age' (4 August 2022), UN Doc A/HRC/51/17, (hereinafter 'Report of the OHCHR, A/HRC/51/17'), undocs.org/A/HRC/51/17.

50 Amnesty International, Privacy International and The Centre for Research on Multinational Corporations (SOMO), 'Operating from the Shadows: Inside NSO Group's Corporate Structure' (2021), privacyinternational.org/sites/default/files/2021-06/DOC1041822021EN.pdf.

51 Delanie Woodlock, 'The Abuse of Technology in Domestic Violence and Stalking' (2017) 23(5) *Sage Journals* 584, doi.org/10.1177/1077801216646277;

DCAF, 'Gender Equality, Cybersecurity, and Security Sector Governance' (2023), www.dcaf.ch/sites/default/files/publications/documents/Gender_Cybersecurity_report_Jan2023.pdf.

52 The right to privacy in the digital age, UNGA Res 75/176, 16 December 2020, undocs.org/A/RES/75/176.



Biometric Surveillance

In addition to communication surveillance, biometric surveillance is a type of activity offered by private surveillance providers that particularly affects the human right to privacy. While communication surveillance targets the exchange of information and data, biometric surveillance refers to a process that collects unique data specifically on the physiological and behavioural characteristics of individuals. These may include fingerprints; voice, face, retina and iris patterns; hand geometry; gait; or DNA profiles. These are widely used by corporate and government agencies around the world for a range of applications, including access control, proof of identity, or for access to services. For surveillance, fingerprints, face data or other biometric data may be used either to compare an individual's characteristics against those stored elsewhere (eg, to access a passport control gate), or to identify someone from within a database of multiple profiles. Facial recognition technologies are increasingly used for mass biometric surveillance in public spaces.⁵³

The right to privacy, including data protection, requires enhanced protections of an individual's sensitive (ie biometric) data. Unlawful biometric surveillance would amount to a serious violation of the right to privacy. The intimate and high-risk nature of biometric data collection can result in particularly negative consequences for individuals when it is misused. For this reason, the processing of biometric data requires stricter limitations and safeguards as compared to other types of data. Private surveillance companies often facilitate the use of biometric technologies by developing, selling or implementing these systems. These entities and their practices are often overlooked by regulatory and judicial systems, as we shall see, due to a lack of regulatory capacity or gaps in regulatory frameworks. This results in private surveillance companies and their clients' operating outside of human rights requirements and the rule of law. The UN Special Rapporteur on counterterrorism and human rights recommended that 'States must make sure that biometric data falls within the scope of data protection laws and that relevant protection is not unduly restricted even when such data is collected, retained, processed or shared in a national security context.'⁵⁴

53 PI, 'Facial Recognition', [privacyinternational.org/learn/facial-recognition](https://www.privacyinternational.org/learn/facial-recognition); PI, 'Mass Surveillance', [privacyinternational.org/learn/mass-surveillance](https://www.privacyinternational.org/learn/mass-surveillance).

54 Dr Krisztina Huszti-Orbán and Prof Fionnuala Ní Aoláin, 'Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?', Report prepared under the aegis of the Mandate of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (2020), www.law.umn.edu/human-rights-center/research/use-biometric-data-identify-terrorists.

PRIVATE SURVEILLANCE AND OTHER HUMAN RIGHTS

As mentioned in the introduction to this section, interference with privacy often opens the gate to other human rights violations. Violations of the right to privacy could allow malicious actors to locate individuals and murder them, for example. Private surveillance activities can impact the rights to freedom of expression, freedom of assembly and association, as well as the rights to life, to liberty and security of the person, to fair trial and due process, the right to freedom of movement, the right to enjoy the highest attainable standard of health and to have access to work and social security.⁵⁵ When surveillance services are used for security purposes, the aforementioned rights are particularly affected.

The Impact of Private Surveillance on the Right to Life

The right to life is a fundamental human right enshrined in both the ICCPR (Article 6) and the ECHR (Article 2). It is a cornerstone of human dignity and freedom, and its protection is essential for the enjoyment of other rights and freedoms. The right to life requires that the state take appropriate measures to protect the lives of everyone under its jurisdiction, including by offering them protection from arbitrary and extrajudicial killings.

The rise of surveillance technologies and the increasing use of them by both the state and private surveillance companies pose a significant threat to the right to life. Surveillance can be used to spy on, to locate, to track and, ultimately, to arrest, to kill or to disappear people. The UN Special Rapporteur on freedom of expression has highlighted:

Surveillance of specific individuals – often journalists, activists, opposition figures, critics and others exercising their right to freedom of expression – has been shown to lead to arbitrary detention, sometimes to torture and, possibly, to extrajudicial killings.⁵⁶

In 2018, this was demonstrated with the murder of a Saudi journalist, Jamal Khashoggi, in Istanbul, which was linked to the use of spyware. The mobile (cell) phones of family members and close friends had reportedly been affected by NSO Group's Pegasus spyware.⁵⁷ The UN High Commissioner for Human Rights has also warned of the dangers of targeted hacking, which has been linked to extrajudicial killings.⁵⁸ (See also Example 8.)

Example 8 | Country Case Study - Libya

In Libya, in 2007, French technology firm Amesys supplied sophisticated communications surveillance systems to the Libyan intelligence services. The systems allegedly permitted the interception of all country-wide, online and phone communications, and the subsequent processing of collected data. Under the Regime of Muammar Gaddafi, the technology became a weapon that facilitated the targeting, arrest and imprisonment of thousands of people in Libya. In 2011, the International Federation for Human Rights (FIDH) and La Ligue des Droits de l'Homme (LDH) brought a criminal case against Amesys for complicity with human rights abuses committed by the Gaddafi regime in Libya because they provided surveillance equipment to the regime.⁵⁹ Subsequent revelations revealed a contract concluded by Amesys – then Nexa Technologies – with the Egyptian regime, in 2014. FIDH and LDH, with the support of the Cairo Institute for Human Rights Studies (CIHRS), filed a complaint. A judicial investigation was opened one month later, in December 2017.⁶⁰

⁵⁵ Ibid.

⁵⁶ Report of the Special Rapporteur, A/HRC/41/35.

⁵⁷ CitizenLab, 'The Kingdom Came to Canada How Saudi-Linked Digital Espionage Reached Canadian Soil' (1 October 2018), citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/; Martin Chulov, 'Jamal Khashoggi: murder in the consulate' The Guardian (21 October 2018), www.theguardian.com/world/2018/oct/21/death-of-dissident-jamal-khashoggi-mohammed-bin-salman.

⁵⁸ Report of the OHCHR, A/HRC/51/17, para 5.

⁵⁹ FIDH, 'Surveillance and torture in Egypt and Libya: Amesys and Nexa Technologies executives indicted', 22 June 2021, www.fidh.org/en/region/north-africa-middle-east/egypt/surveillance-and-torture-in-egypt-and-libya-amesys-and-nexa

⁶⁰ Ibid. See further developments, FIDH, 'Surveillance and torture in Libya: The Paris Court of Appeal confirms the indictment of Amesys and its executives, and cancels that of two employees', 22 November 2022, www.fidh.org/en/impacts/Surveillance-torture-Libya-Paris-Court-Appeal-indictment-AMESYS

It is crucial to address these concerns and to ensure that the use of surveillance technologies is properly regulated to prevent violations of the right to life. The systemic violation of an individual's or a community's right to life highlights the grave consequences of insufficient regulation of the private security sector. This requires clear legal frameworks and strong oversight mechanisms to ensure that these technologies are used in a manner that is compatible with human rights. The protection of the right to life is essential for the enjoyment of other rights and freedoms, and its protection must be a priority in any discussion of surveillance and privacy.

The Risks to the Rights to Freedom of Expression, Assembly and Association under Private Surveillance

The right to freedom of expression is a cornerstone of democracy, and it is guaranteed under several international and regional charters, including Article 19 of the Universal Declaration of Human Rights (UDHR) and Article 18 of the ICCPR.⁶¹ This right encompasses the freedom to exchange information and ideas privately. It also requires that communications be received only by their intended recipient, without tampering or inspection by a third party. Further, it affirms the right of individuals to hold opinions, and to share and to receive information of all kinds through any medium, regardless of frontiers.⁶² Similarly, the rights to freedom of assembly and association, protected under Article 20 of the UDHR and Article 21 of the ICCPR, are key elements in every society, democratic or otherwise.⁶³

However, the increasing use of surveillance technologies by both the state and private surveillance companies puts at risk the enjoyment of internationally recognised rights. Many individuals, including political opponents, dissidents, journalists, activists and groups, face violations of their rights when their communications, movements and activities are tracked. The UN Special Rapporteur on the promotion and protection of the right

to freedom of opinion and expression has concluded that 'interference with privacy through targeted surveillance is designed to repress the exercise of the right to freedom of expression'.⁶⁴ This is undermining the very essence of the right to freedom of expression. Likewise, communications surveillance and other surveillance practices, carried out by governments or private actors, may directly infringe on people's freedom of peaceful assembly.⁶⁵ The UN High Commissioner for Human Rights has concluded that 'the use of [new] technologies to surveil or crack down on protesters can lead to human rights violations, including infringement of the right to peaceful assembly'.⁶⁶

Freedom of expression includes the right to remain anonymous. This is an element that is particularly essential for journalists when collecting unbiased and transparent information from sources. In environments subject to regular unlawful surveillance, both biometric and communications-based, sources may censor or falsify the reports they provide to journalists or refuse to participate in interviews. Also, unlawful surveillance hampers the rights to the freedoms of assembly, association and expression when the 'civic space' in which individuals may convene to exchange ideas and information becomes increasingly limited.⁶⁷ The mere fact that surveillance is suspected could discourage individuals from meeting, assembling or exchanging information.

Many private surveillance companies provide services to states that use them to monitor journalists, human rights defenders and political opponents. Biometric and communication surveillance technologies can, for example, be used to harass individuals or groups, to perform internet shutdowns or to block websites. If diverse actors are systematically surveilled and censored, a community's collective rights to expression, assembly and association are abused, as these diverse perspectives are eliminated and their accounts silenced. For these reasons, states must recognise the significant role that private surveillance providers can play in the provision of the right to freedom of expression, as well as the rights to freedom of association and assembly.

61 UDHR, ratified by UNGA Resolution 217A, 10 December 1948. See also Article 10 ECHR; Article 13 ACHR; Article 9 of the African Charter on Human and Peoples' Rights (ACHPR).

62 UNHRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (17 April 2013), UN Doc A/HRC/23/40, undocs.org/A/HRC/23/40.

63 See also Article 19 ECHR; Articles 15-16 ACHR; Articles 10-11 ACHPR.

64 Report of the Special Rapporteur, A/HRC/41/35, para 21.

65 Iliia Siatitsa, 'Freedom of assembly under attack: General and indiscriminate surveillance and interference with internet communications' (2021) 102(913) *IRRC* 181, international-review.icrc.org/articles/freedom-assembly-under-attack-surveillance-interference-internet-communications-913#footnoteref1_qyjmesp.

66 UNHRC, 'Report of the United Nations High Commissioner for Human Rights on the impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests' (24 June 2020) UN Doc A/HRC/44/24, undocs.org/A/HRC/44/24.

67 PI, 'Protecting civic spaces' (2019), privacyinternational.org/long-read/2852/protecting-civic-spaces.

Impact of Private Surveillance on the Right to Non-Discrimination

If the rule of law is to be implemented consistently, laws must be based on fair and equitable principles, and all must be accountable under these laws without discrimination. Article 26 of the ICCPR provides that 'All persons are equal before the law and are entitled without any discrimination to the equal protection of the law.'⁶⁸ In the Declaration of the High-Level Meeting of the General Assembly on the Rule of Law, member states affirmed these principles by committing to 'respect the equal rights of all without distinction as to race, sex, language, or religion'.⁶⁹

However, many surveillance technologies developed and implemented by private companies can be used to target individuals for monitoring, or even detention, based on their social origin, ethnicity, perceived behaviour or appearance, amongst other factors. For instance, WeChat is a Chinese multi-purpose messaging, social media and mobile-payment app. As of 2013, it was being used by around one million Uighurs, but in 2014, WeChat was forced to allow the Chinese Government to monitor people's conversations.⁷⁰ The data collected, combined with the technology deployed, has allowed the authorities to comprehensively track and control the Uighur population. This surveillance has facilitated the arrest and detention of around one million people in 're-education' camps as of 2018.⁷¹

Biometric surveillance can be particularly concerning in this regard, as many systems rely on predictive technologies, and they are susceptible to both human and machine error. For example, human subjectivity or mistakes when constructing categories used to classify or evaluate individuals, may perpetuate stereotypes or lead to discrimination. In practice, the UN Special Rapporteur on contemporary forms of racism highlighted a biometric surveillance system that was not programmed with all possible dialects of Arabic, leading to potentially erroneous and biased targeting of perceived 'non-credible' individuals based on a lack of recognition of their spoken language.⁷²

Biometric surveillance technologies themselves can similarly violate the right to non-discrimination when, amongst other things, they misidentify people or information. Some programs are particularly inaccurate in identifying members of a certain race, ethnicity or group. This results in further discrimination.⁷³ Thus, private surveillance companies play a significant role in ensuring the provision of both the equitable rule of law and a society's right to non-discrimination. Quite often, these technologies are rolled out in particularly precarious situations: a pertinent example is that concerning border controls, through which people in vulnerable positions, such as migrants, pass every day,⁷⁴ without having been tested beforehand and without any appropriate remedial mechanisms in place.⁷⁵ Furthermore, AI-enabled technology has the risk of amplifying bias, leading to discrimination (see Example 9).⁷⁶

68 See also, indicatively, the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD); Article 14 ECHR.

69 Declaration of the high-level meeting of the General Assembly on the rule of law, 30 December 2012, UN Doc A/RES/67/1, para 3.

70 Ricardo Weibezahn, 'How China Targets Uighurs "One by One" for Using a Mobile App', International Consortium of Investigative Journalists, 24 November 2019, www.icij.org/investigations/china-cables/how-china-targets-uighurs-one-by-one-for-using-a-mobile-app/.

71 Darren Byler, 'China's hi-tech war on its Muslim minority', 11 April 2019, www.theguardian.com/news/2019/apr/11/china-hi-tech-war-on-muslim-minority-xinjiang-uighurs-surveillance-face-recognition.

72 UNHRC, 'Report of the UN Special Rapporteur on contemporary forms of racism on contemporary forms of racism, racial discrimination, xenophobia and related intolerance' (10 November 2020), UN Doc. A/75/590, para 25, documents-dds-ny.un.org/doc/UNDOC/GEN/G21/285/95/PDF/G2128595.pdf.

73 Ibid para 9.

74 OHCHR and University of Essex, 'Study on Digital Border Governance: a Human Rights Based Approach' (18 September 2023), www.ohchr.org/en/documents/tools-and-resources/digital-border-governance-human-rights-based-approach.

75 UNHRC, 'Report of the Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination on impact of the use of private military and security services in immigration and border management on the protection of the rights of all migrants' (9 July 2020), UN Doc A/HRC/45/9, undocs.org/A/HRC/45/9.

76 OHCHR and University of Essex, 'Study on Digital Border Governance: a Human Rights Based Approach' (18 September 2023), www.ohchr.org/en/documents/tools-and-resources/digital-border-governance-human-rights-based-approach; ODIHR, 'Policy Brief: Border Management and Human Rights Collection, processing and sharing of personal data and the use of new technologies in the counter-terrorism and freedom of movement context' (2021) at 24.

Example 9 | Women's and LGBTQ+ Rights

Surveillance subjects women and LGBTQ+ communities to higher risks of discrimination and harm. According to the UN General Assembly, violence against women is defined as 'any act of gender-based violence that results in, or is likely to result in, physical, sexual or psychological harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life'. This includes 'physical, sexual and psychological violence perpetrated or condoned by the State, wherever it occurs'.⁷⁷ Surveillance targeted at women can have particularly serious effects, 'given that political, societal, and gender power asymmetries often grant authorities opportunities to weaponize the information they extract through defamation, blackmail, and doxxing. This can include the publishing of private and intimate photos and conversations online.'⁷⁸ Surveillance technologies and services are also used to target LGBTQ+ communities. In one example, there are some specific biometric tools that aim to recognise homosexual people. Recently, it was reported that Grindr, a networking app for LGBTQ+, was allegedly used by authorities in Egypt to persecute these communities.⁷⁹

Safeguarding the Right to a Fair Trial

The UDHR affirms that everyone is entitled to a 'fair and public hearing by an independent and impartial tribunal', and that they must be 'presumed innocent until proved guilty according to law'.⁸⁰ The right to a fair trial is further protected by international and regional treaties.⁸¹ Despite this guarantee, many private surveillance companies and their clients rely on predictive models to build communication and biometric monitoring systems. These models negate the presumption of innocence, and this often leads to profiling based on inaccurate and discriminatory biases. 'Behaviometrics' enabled by biometric technologies can have similar negative consequences on the right to a fair trial. This becomes particularly true when used in detention and in interrogation contexts to make assumptions based on a person's perceived behaviours or emotions.⁸² Similarly, many illicit surveillance practices negate the principle that offences and penalties must be defined by law, since the factors being monitored are typically not publicised.⁸³ All of these weaken the transparency and equity that underlie a fair judicial and legislative system.

77 Declaration on the Elimination of Violence against Women, UNGA Resolution 48/104, 1993, undocs.org/A/RES/48/104.

78 Access Now and Front Line Defenders, 'Unsafe anywhere: women human rights defenders speak out about Pegasus attacks' (17 January 2022), www.accessnow.org/women-human-rights-defenders-pegasus-attacks-bahrain-jordan/.

79 European Digital Rights (EDRI), 'The digital rights of LGBTQ+ people: When technology reinforces societal oppressions' (17 July 2019), edri.org/our-work/the-digital-rights-lgbtq-technology-reinforces-societal-oppressions/.

80 Articles 10-11 UDHR, above.

81 Indicatively, Article 14 ICCPR; Article 6 ECHR; Article 8 ACHR.

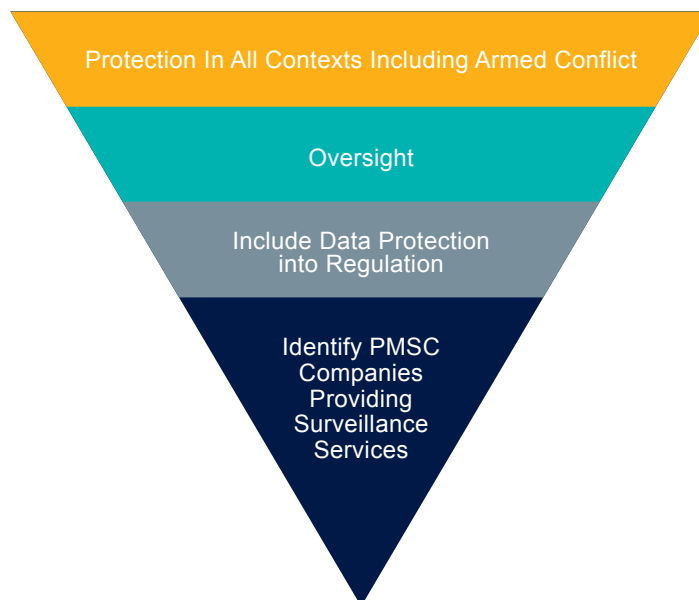
82 Statement by Special Rapporteur on the Promotion and protection of human rights and fundamental freedoms while countering terrorism, 29 June 2021, www.un.org/counterterrorism/sites/www.un.org/counterterrorism/files/210729_session_iii_professor_ni_aolain_statement.pdf

83 UNGA, Report of the Special Rapporteur on contemporary forms of racism, 10 November 2020, UN Doc A/75/590, para 25. undocs.org/A/75/590

THE PERTINENCE OF THE EXISTING PRIVATE MILITARY AND SECURITY COMPANIES REGULATORY FRAMEWORK FOR PRIVATE SECURITY COMPANIES PROVIDING SURVEILLANCE SERVICES

This section looks at how existing international norms and good practices for private security regulation (namely, the Montreux Document, the International Code of Conduct and the UN Guiding Principles on Business and Human Rights) can serve as a basis for strengthening the regulation of some private surveillance providers and technologies.

INTEGRATING SURVEILLANCE SERVICES INTO PMSC REGULATION



To improve governance of private security companies providing surveillance services – and thus increase the protection of human rights – a more thorough and systematic understanding of the industry’s landscape, technology and key stakeholders must be reached beyond this report’s overview. Preventing and dealing with private surveillance’s impact on human rights requires an understanding of how complex technologies work. As technology continuously advances and evolves, so do the capabilities and services of private security companies. Security-sector governance actors require up-to-date skills to understand, monitor and oversee private surveillance services. In addition, safeguards against abuse must be put in place to ensure effective oversight of these services. Moreover, the extraterritorial reach and/or export of private surveillance presents a distinct set of governance and oversight challenges.

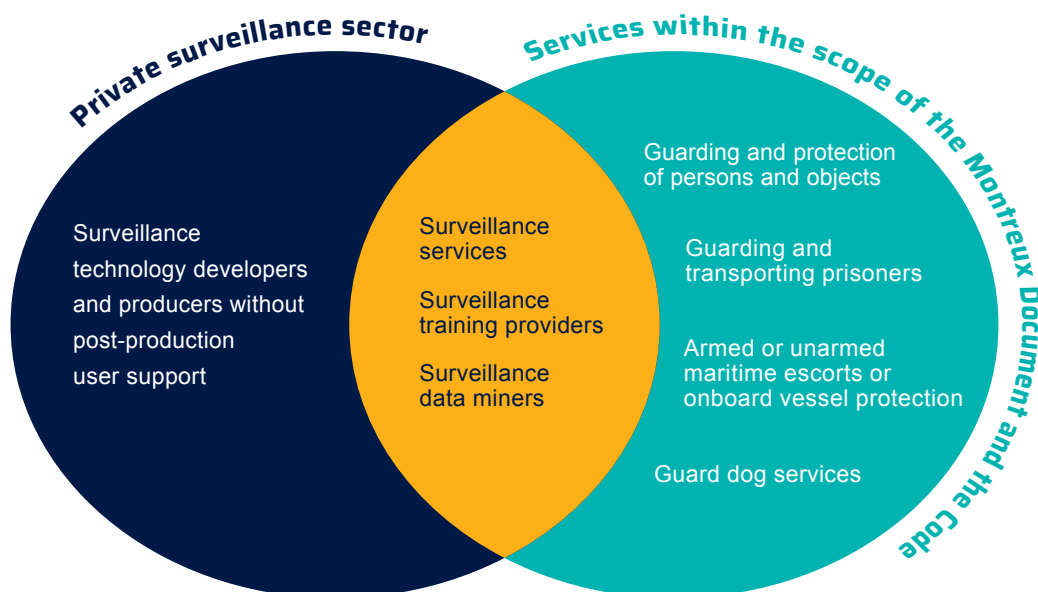
The existing PMSC regulatory framework provides norms, good practices, guidance and tools when addressing these gaps. Since 2008, the Montreux Document has reaffirmed the existing obligations of states under international law; in particular, international humanitarian law and international human rights law when related to the activities of private military and security companies (PMSCs). The International Code of Conduct for Private Security Service Providers (the Code) articulates responsibilities of private security companies under human rights and international humanitarian law to ensure the responsible provision of private security services, particularly when operating in complex environments. The following subsections show how the Montreux Document, the International Code of Conduct for Private Security Service Providers, the UN Guiding Principles on Business and Human Rights and other standards offer responses for improving governance of private surveillance.

IDENTIFYING PRIVATE SECURITY COMPANIES PROVIDING SURVEILLANCE SERVICES

For the purposes of this policy paper, surveillance companies are understood as companies that market hardware and software for the explicit purpose of conducting surveillance for law enforcement, intelligence or security purposes.⁸⁴ Understanding the private surveillance landscape is key to identifying private security companies who, in turn, provide surveillance services. By sizing up surveillance capabilities, such companies' impact on human rights can be anticipated. As mentioned previously, private security companies providing surveillance services do not include the entire spectrum of companies providing surveillance technologies. However, in practice, technology providers are difficult to differentiate from service providers. This is because, in some cases, technology developers will offer services to support the use of their product. Regardless, the Montreux Document provides an inclusive definition of a 'private and military security company'.⁸⁵ This definition encompasses companies that provide either military or security services or both, including surveillance services. The relevant question is not how a company is labelled, but what specific services it provides in a particular instance. The Code includes in the category of 'security services' operational and logistical support for armed or security forces. This encompasses training and advice, intelligence, surveillance and reconnaissance activities.

Therefore, it is safe to state that private surveillance activities are covered by existing private security governance frameworks. The exact scope of the private surveillance companies to be incorporated needs to be continuously defined as technological capabilities continue to develop. Private security stakeholders, addressing state actors and civil society, need to be aware of the varied range of services that could be considered as private security to avoid gaps of accountability and oversight. Such awareness raising would enable increased protection of the human rights affected by these types of services. Private surveillance companies develop and use a great variety of technologies to intercept communications and access data – either while the data is stored or being exchanged, or afterwards. In addition, equipment allows for collecting and for sorting through biometric data online or from devices such as street or surveillance cameras. The fact that new technology is constantly emerging, and that individuals are themselves not aware that their data – be it biometric or other – is accessed makes it difficult to prevent abuse. Access to such technologies and services has allowed state agencies and other parties to identify and to locate individuals. This may then lead to serious human rights violations. In some countries, an export permit will be denied if there is reason to believe that the goods will be used by

EXAMPLES OF SURVEILLANCE SERVICES WITHIN THE SCOPE OF PRIVATE SECURITY INTERNATIONAL NORMS AND GOOD PRACTICES



84 See 'Introduction' to this paper.

85 See Ibid.

the final recipient for repression. In practice, this is very difficult to prove, and it requires a lot of effort to acquire information. The information needs to be concrete enough to hold up in front of the courts. In some regulations, if the export is allowed, usually the services in connection with the export (eg, introductory training) is also allowed.⁸⁶

International private security governance good practices offer guidance on preventing human rights violations. Given the far-reaching implications of private surveillance on human rights, and in order to guarantee that private security companies providing security services do not cause or facilitate human rights abuses, such guidance, among other safeguards, declares that states should ensure:

- ▶ **Identification**, that is, appropriate resources and expertise for PMSC regulators to identify private security companies providing private surveillance through research, studies, mapping and other methods.
- ▶ **Scope of application**, that is, private security regulation that explicitly covers private surveillance services.

PRIVATE SURVEILLANCE SERVICES AND DATA PROTECTION

Data protection standards apply in full to private security companies providing surveillance services. While within the PMSC regulation there are no specific guidelines on data protection, there are other international standards that may provide guidance.⁸⁷ While data protection laws vary from country to country, there are some commonalities and minimum requirements, underpinned by data protection principles and standards which tend to be reflected in the structure and content of relevant legislation.⁸⁸ For example, the processing of personal data by private security companies shall be adequate, relevant and limited to the necessity of the purpose for which it is being processed.⁸⁹ Furthermore, the Montreux Document and the Code's requirements for authorisation, licensing, vetting and training, as well as monitoring and accountability, promote further strengthening of practices to guarantee that such data protection standards are clearly stated, monitored, upheld and remedied in case of breach.

More specifically, states should determine whether compliance with data protection principles should be monitored by the private security regulator or by another authority. In other words, the entity to which data protection policies, security measures and data management plans should be provided needs to be established. To understand the issue of data protection, a comparison with arms control – in countries where private security can carry arms – could increase our understanding of the problem. In contexts where private security carry firearms, some countries choose to oversee private security and arms control separately, while others regulate private security and arms within the same agency. Similarly, overseeing respect for data protection by private surveillance companies could be attributed to private security regulators, or to a distinct entity specialising in data protection. Although it should be noted that it is crucial that coordination between agencies be facilitated to avoid gaps in oversight. To avoid these gaps, states need to ensure that there is:

- ▶ **A legal framework**, that is, a data protection framework in which PMSCs adhere to and comply with the data protection principles.
- ▶ **Sharing of responsibilities**, that is, the the sharing of responsibilities/mandates between PMSC regulators and data protection authorities.
- ▶ **Coordination**, that is, planning and setting up coordination processes between data protection authorities and PMSC regulators to, amongst other things, exchange information and expertise.
- ▶ **Training**, that is, providing data protection specialists with training on the challenges linked to the provision of surveillance services by private security companies. Similarly, private security regulators should receive parallel training with data protection capacity-building.

86 SR 935.411, Ordinance of 24 June 2015 on Private Security Services provided Abroad (OPSA), Article 8a.

87 A representative example of such legislative framework is 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 (General Data Protection Regulation) [2016] OJ L119/1, eur-lex.europa.eu/eli/reg/2016/679/oj.

88 PI, 'Data Protection Guide', privacyinternational.org/data-protection-guide.

89 Ibid. See also EU General Data Protection Regulation, above.



OVERSIGHT OF PRIVATE SECURITY COMPANIES' SURVEILLANCE SERVICES

Monitoring and oversight of private security companies providing surveillance services is the responsibility of the state. To be carried out effectively, oversight requires understanding of the latest technologies used by private surveillance companies, having a strong and independent mandate and an appropriate regulatory framework. International private security governance good practices advise that states get the capacity and the resources to carry out the increasingly complex range of activities required for the effective regulation and monitoring of PMSCs.

According to the Montreux Document, a specific national regulatory authority, tailor-made for the purpose of overseeing private security companies, should be in place. Regarding the effective oversight of private surveillance, this authority should have specific skills and/or employees who can oversee private surveillance companies. In addition, regulatory authorities need to be sufficiently autonomous from other state agencies to avoid the risks of interference, lack of transparency and corruption. Regulators could exercise autonomous oversight to monitor state access to data obtained by or in the possession of private actors. The legal framework should be updated to include special provisions for regulatory requirements on surveillance and data protection and state access to corporate data. Furthermore, ICT4Peace recommends that corporate actors exercise due diligence when being requested to hand over data to states or other actors. This requires private actors to understand what the law requires them to hand over and the extent to which they can refuse such requests.⁹⁰

As seen in many cases, state agencies increasingly rely on private security companies to surveil dissidents, critics and human rights defenders. This may result in serious violations of human rights. For example, authorities may seek to unlawfully access this data and to target individuals, in order to commit human rights violations against them. For this data collection and access, such governments may often resort to the services of private security companies providing surveillance services, allowing them, in certain circumstances, to bypass national surveillance legislation and oversight regulation. In many countries, oversight mechanisms, where they exist, do not have the legal or the administrative capacity to monitor either security and intelligence agencies or private surveillance services to prevent human rights violations. In Nigeria, for example, there is no autonomous body overseeing the activities of investigating authorities.⁹¹ Another example is Kenya, where data protection does not apply to national security.⁹² As a result, authorities may access public and private cameras without oversight, under the pretext of national security.⁹³

Accordingly, it becomes even more essential for the private security regulator to exercise effective oversight of private security companies providing surveillance services. The regulator could exercise scrutiny of data collection and transmission by the private sector. Some countries do ensure transparency in reporting on paper. Brazil's national court publishes a database containing some statistical information about the communications interceptions by the state authorised by the court.⁹⁴

90 Bazatu, 'From Boots on the Ground', above.

91 Ridwan Oloyede, 'Surveillance Law in Africa: a review of six countries Nigeria country report' (2021), opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/16893/Nigeria%20Country%20Report.pdf?sequence=7&isAllowed=y.

92 PI, 'Analysis of Kenya's Data Protection Act 2019' (January 2020), privacyinternational.org/sites/default/files/2020-02/Analysis%20of%20Kenya%20Data%20Protection%20Act%2C%202019_Jan2020.pdf.

93 Grace Mutung'u, 'Surveillance Law in Africa: a review of six countries Kenya country report' (2021), opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/16893/Kenya%20Country%20Report.pdf?sequence=6&isAllowed=y.

94 Katizia Rodriguez et al, 'The State of Communication and Privacy Laws in Brazil' (2020) necessaryandproportionate.org/country-reports/brazil/twenty-twenty/.

The Digital and Freedom Bill currently being reviewed in the Nigerian parliament would seek to make it compulsory for private providers to publish government requests for data.⁹⁵ The laws of different countries differ in terms of the extent of operations that are allowed without a court order, but many are unclear about the circumstances that justify such operations. Even if some states effectively oversee the activities of private security companies that are providing surveillance services under their territorial jurisdiction, they may not always control the human rights implications of such companies' activities abroad.

Many countries simply have no restrictions on entities conducting electronic surveillance outside their borders. Private security good practices recommend either that PMSC-relevant legislation should specify that PMSCs' operations abroad fall under their jurisdiction, or that states should adopt specific legislation relating to the activities of PMSCs abroad. Good practices also recommend cooperation between states to reduce such accountability gaps at the transnational level. The Vodafone case study demonstrates how surveillance technology and services can be used freely by states to commit human rights abuses. Furthermore, as explained, surveillance practices present differentiated risks according to gender and sexual orientation, so oversight must address these differences. States must regulate PMSCs, unlawful discrimination and sexual offences. And, for this reason, they must understand the ways in which surveillance exposes population groups differently to such risks.⁹⁶

In order to tackle such complexity, it would be useful for countries to share information and good practices on a dedicated platform. The Montreux Document Forum and the International Code of Conduct Association would be natural fora for such platforms.

To effectively oversee private security companies' surveillance services and to protect human rights, states should safeguard the following aspects of the private security regulatory authority:

- ▶ **Mandate**, so that it oversees both the public and the private use of private surveillance services.
- ▶ **Autonomy**, so that it has the level of autonomy necessary to oversee private surveillance services.
- ▶ **Assessment**, so that it carries out an assessment of the private security regulator's staff capacities regarding surveillance services provided by private security companies.

- ▶ **Training**, so that it receives training in human rights obligations and the implications of surveillance services.
- ▶ **Licensing**, so that there is a transparent authorisation and licensing process to be followed by private security companies providing surveillance services, with clear criteria (eg, no reliably attested record of involvement in serious crime).
- ▶ **Scope of oversight**, to ensure that private security companies providing surveillance services take, amongst others, the following steps:
 - provide transparent reporting of the content of services, technology and equipment used;
 - conduct human rights impact assessments of surveillance services;
 - adopt clear personnel vetting rules to establish which private companies are suitable for carrying out private surveillance and for what purpose;
 - provide adequate and continuous training for employees of private surveillance services on human rights and humanitarian law; and
 - monitor compliance and provide accountability as well as effective remedies in cases of misconduct.
- ▶ **Transparency**, to establish that reports are published containing statistical information about data requests made to private security companies who provide surveillance services.
- ▶ **Public-private collaborations**, to clarify exact conditions whereby public authorities can request information from private security companies providing surveillance services.
- ▶ **Extraterritorial oversight**, to establish whether private security offering surveillance services abroad fall under the regulator's jurisdiction, or whether specific legislation needs to be adopted relating to the activities of private security offering surveillance services abroad.
- ▶ **Participation in private security governance fora**, that is, participation in private security governance fora for states, such as the Montreux Document Forum and/or the International Code of Conduct Association, to coordinate and to share information across borders.

⁹⁵ Ibid.

⁹⁶ DCAF, OSCE/ODIHR, UN Women, Policy Brief Guidance: Gender and Private Security Regulation, 2019.

Private Security Companies' Surveillance Services in Situations of Armed Conflict

Private security companies are increasingly involved in situations of armed conflict. Private surveillance companies are also increasingly involved in situations of armed conflict, which can have adverse impacts for those involved or caught in the crossfire. Additionally, it can raise jurisdictional questions in the conflict zones in which they operate.

The PMSC regulatory framework offers some guidance with relation to the assessment of private security companies providing surveillance services in armed-conflict situations. Specifically, the Montreux Document recalls that states have an obligation to refrain from encouraging or from assisting in violations of international humanitarian law by any party to an armed conflict.⁹⁷ Furthermore, the Montreux Document and the Code acknowledge that private security clients (states or others) can affect respect for international humanitarian law. When selecting and contracting companies, clients can influence how PMSCs operate in the field. Both documents highlight that clients must ensure that the PMSCs they contract and their personnel are aware of their obligations when they are deployed to conflict situations, and that they are trained accordingly.⁹⁸

However, similar to other situations, little attention has been given to the regulation and to the oversight of private security companies providing surveillance services in a situation of armed conflict. The PMSC regulatory framework offers the basis for taking necessary measures to ensure the PMSCs' compliance with international humanitarian law and international human rights law.

Therefore, in relation to armed conflict, states should also ensure the following aspects of PMSC regulators:

- ▶ **Assessments**, that is, in situations where private surveillance services provided by private security companies have a high probability of being used in armed conflicts, conduct assessments of the corresponding impact on international humanitarian law and human rights law.
- ▶ **Regulatory framework**, that is, clarify the rules and restrictions on surveillance services provided by private security companies in the context of an armed conflict.
- ▶ **Monitoring**, that is, monitor activities of private surveillance services provided by private security companies abroad through reporting requirements and/or through cross-border cooperation.

⁹⁷ For example, Montreux Document, para 9(b).

⁹⁸ For example, Montreux Document, para 3(a).



CONCLUDING OBSERVATIONS

This paper has sought to highlight the potential for the existing international PMSC regulatory framework to support more effective regulation of private surveillance services. It has provided a brief overview of different private surveillance technologies and services, to assist with the evaluation of the extent to which they could be seen as private security providers. It has further underlined the serious human rights impacts that private surveillance services may have. Moreover, it has demonstrated that existing frameworks do indeed apply to private surveillance services as well, and it offers effective guidance to improve private security governance in this area. Accordingly, there is a need for international initiatives, industry stakeholders and states to convene in determining how to concretely improve privatised surveillance governance based on the Montreux Document and the International Code of Conduct for Private Security Service Providers.

The Montreux Document and the Code implementation efforts should actively incorporate private surveillance for outreach, legal and policy reform, and capacity-building efforts, including, amongst others:

- ▶ **Guidance.** This includes specific guidance for integrating private security companies' surveillance services in private security regulation and oversight. Accountability mechanisms should be developed and adapted to different audiences (regulators, states, civil society organisations, clients). For instance, the Montreux Document

Forum could develop interpretative guidance for the Montreux Document regarding private security companies who provide surveillance services.

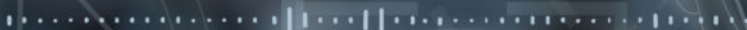
- ▶ **Advisory support.** Private security regulatory and advisory support to states should include an element on private surveillance.
- ▶ **Capacity building.** All stakeholders should be trained for the human rights risks and impacts of privatised surveillance activities.
- ▶ **Awareness raising.** Outreach activities should highlight the relevance to all stakeholders of the Montreux Document and the Code for regulation of privatised surveillance. In example, state agencies, the industry, civil society, and clients.
- ▶ **ICoCA reporting.** Member companies of the International Code of Conduct Association (ICoCA) should report compliance with data protection to the ICoCA.
- ▶ **Certification.** Data protection should be included more prominently as part of private security certification processes such as PSC.1, ISO 18788, ISO 28007.





15098 4
11 75 19
734 00 5
756
67

8374 001 991



DCAF Geneva Centre
for Security Sector
Governance



**Maison de la Paix
Chemin Eugène-Rigot 2E
CH-1202 Geneva, Switzerland
Tel: +41 22 730 94 00
info@dcaf.ch
www.dcaf.ch**

**62 Britton Street,
London, EC1M 5UY
UK**