SAFEGUARDS FOR PUBLIC-PRIVATE SURVEILLANCE PARTNERSHIPS

December 2021

privacyinternational.org

ABOUT PRIVACY INTERNATIONAL

Governments and corporations are using technology to exploit us. Their abuses of power threaten our freedoms and the very things that make us human. That's why Privacy International campaigns for the progress we all deserve. We're here to protect democracy, defend people's dignity, and demand accountability from the powerful institutions who breach public trust. After all, privacy is precious to every one of us, whether you're seeking asylum, fighting corruption, or searching for health advice.

So, join our global movement today and fight for what really matters: our freedom to be human.

Privacy International
62 Britton Street, London EC1M 5UY, United Kingdom
Phone +44 (0)20 3422 4321
privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).

CONTENTS

INTRODUCTION

As states around the world seek to expand their surveillance capabilities and harness the power of data to deliver public services, they are often tempted to use the services of private technology companies – through public-private partnerships ('**PPPs**'). The fight against COVID-19, and associated urgency to find answers and solutions, has only increased the perceived need for states to use 'innovative' technologies and big data analytics systems developed by companies. But these PPPs are taking on a new form, diverging from traditional public procurement relationships. We observe much more co-dependency between the parties, whereby the state may be developing new systems or processes entirely reliant on the services of one company, and the company may be receiving access to data or other information for use in developing its own services. Beyond a simple "one-off" commercial relationship, these partnerships are often built over courting, promises of attaining perfect truth, and ever more private access to data – often circumventing public procurement rules and impeding on fundamental rights in the process.

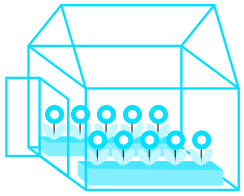
The privatisation of public responsibilities can be deeply problematic if deployed without the safeguards required to ensure human rights are not quietly abused. This is particularly true when the systems deployed are used for surveillance and mass processing of personal data. Private companies have been known to play with the limits of what can legally and ethically be done with individuals' identities and data, without the same level of accountability required of public authorities – a significant affront to fundamental rights when used to deliver a public service.

Through our investigative work and the work of our partners around the world, PI has identified a number of issues common to PPPs that involve surveillance technology and/or the mass processing of data. To address these issues, we have defined corresponding safeguards that we recommend for implementation by public authorities and companies who intend to enter into such partnerships. Classified between principles of Transparency, Adequate Procurement,

Accountability, Legality, Necessity & Proportionality, Oversight and Redress, together they seek to uphold human rights and restore trust in the state's public functions as these increasingly get outsourced to private hands. The safeguards intend to be jurisdiction-blind, so that they can apply as widely as possible across the globe. They are a living document, which we update regularly with new examples of abuse from across the world and of successful advocacy against surveillance partnerships.

The United Nations Guiding Principles on Business and Human Rights (the '**UN Guiding Principles**'),[1] unanimously endorsed by states through the UN General Assembly in 2011,[2] provide a clear mandate for states and companies alike to step up measures to respect, protect and fulfil human rights and fundamental freedoms, and to extend their responsibilities in this regard, including in the technology industry.[3] The following safeguards outline what PI believes to be a reasonable framework of protections to enforce these responsibilities, and ensure that PPPs do not result in human rights abuses. PI hopes that this outline can help civil society and communities advocate for such a scheme when faced with ubiquitous deployments of technology.

[1] Office of the UN High Commissioner for Human Rights, Guiding Principles on Business and Human Rights, 2011, available at https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf.
[2] UN Human Rights Council Resolution on Human Rights and transnational corporations and other business enterprises, UN Doc A/HRC/RES/17/4, 6 July 2011, available at https://undocs.org/en/A/HRC/RES/17/4.
[3] Application of the UN Guiding Principles to the technology industry was reaffirmed by the UN High Commissioner for Human Rights in the B-Tech Foundational Paper on The UN Guiding Principles in the Age of Technology, available at https://www.ohchr.org/Documents/Issues/Business/B-Tech/introduction-ungp-age-technology.pdf.

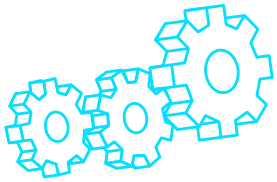


TRANSPARENCY

Public-private partnerships and the technologies they deploy are often very opaque, with states and companies withholding excessive information. But transparency is essential to enable scrutiny of the exercise of a state's powers, and is a precondition to any challenge of authority and assertion of rights.

ADEQUATE PROCUREMENT

States ought to adhere to certain formal processes for procuring and assessing the services of private companies for delivery of public duties. Through such processes, both the state and the company ought to perform due diligence on each other to ensure they comply with their respective human rights obligations, at every stage of a partnership's lifecycle.



ACCOUNTABILITY

Accountability means [1] defining the responsibilities of each party in a partnership - identifying obligations, duties and standards, and [2] designing mechanisms enabling third parties to scrutinise and challenge its consequences.

As states around the world seek to expand their surveillance capabilities and harness the power of data to deliver public services, they are often tempted to use the services of private technology companies – through public-private partnerships ('PPPs').

Through our investigative work and the work of our partners around the world, PI has identified a number of issues common to PPPs that involve surveillance technology and/or the mass processing of data.

SA[illegible]IPS

The privatisation of public responsibilities can be deeply problematic if deployed without the safeguards required to ensure civil liberties and human rights are not quietly abused. This is particularly true when the systems deployed are used for surveillance and mass processing of personal data.

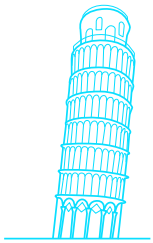
To address these issues, we have defined corresponding safeguards that we recommend for implementation by public authorities and companies who intend to enter into such partnerships. Classified between six principles, together they seek to uphold human rights and restore trust in the state's public functions.

LEGALITY, NECESSITY AND PROPORTIONALITY

The use of a private technology or system to deliver public functions must be legal, necessary to achieve a defined goal, and proportionate (any adverse impact on citizens' rights and freedoms must be justified). Any partnership must be able to show that legality, necessity and proportionality assessments have been performed.

OVERSIGHT

A partnership and the technologies it deploys must be subject to continued independent oversight, to ensure they remain circumscribed to their stated purpose, to detect abuses or resulting harm, and to require redress.



REDRESS

Parties affected by a partnership's technology must have avenues for redress. Redress mechanisms must assign responsibility between the state and the company involved in a partnership, and provide both non-judicial and judicial avenues to raise and resolve adverse human rights impacts.

I. TRANSPARENCY

Transparency is core to and a preliminary requirement of any exercise and protection of human rights. Without appropriate transparency, the exercise of a state's powers cannot be subject to proper public scrutiny. The UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has observed that "[t]he principle of transparency and integrity requires openness and communication about surveillance practices." The Special Rapporteur also noted that "[o]pen debate and scrutiny is essential to understanding the advantages and limitations of surveillance techniques, so that the public may develop an understanding of the necessity and lawfulness of surveillance."[4]

PPPs, and the ongoing commercial relationship they set up, often suffer from a lack of transparency. Companies have commercial interests in preserving confidentiality in their proprietary systems and algorithms – and we have often seen states liberally use that justification to withhold as much information as possible about details of a surveillance or data analytics technology. But just like any public procurement process, PPPs require transparency at every step of their deployment – from public tender processes to policies around deployment of technologies, to the impact or results of deployments. This is essential for the public and civil society to grasp the extent of and the modalities of surveillance and government through data.

	Issue	Example(s)	Safeguard(s)
1	Very limited information publicly accessible – painstaking efforts from CSOs are	Palantir and the UK government: information about Palantir's collaboration	**All PPP documentation should be made publicly available** – and where legitimate concerns around disclosure of sensitive information arise (such as state

[4] Report of the UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, A/HRC/13/37, 28 December 2009 ("2009 Report of the UN Special Rapporteur on Counter Terrorism"), paras 54 and 56, available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G09/178/04/PDF/G0917804.pdf?OpenElement; see also *Escher et al. v. Brazil*, Inter-American Court of Human Rights, Judgment (on Preliminary Objections, Merits, Reparations, and Costs), Concurring Opinion of Judge Sergio García Ramírez, Series C No. 200, 6 July 2009, para. 6 ("We reject the furtiveness with which the tyrant hides his intolerable arbitrariness. We condemn the secrecy that shrouds the symbols of authoritarianism. We censure opacity in the exercise of public authority. We demand – and we are achieving, step by step, based on the argument of human rights – transparency in the acts of Government and in the conduct of those who govern us.").

	Issue	Example(s)	Safeguard(s)
	required to obtain limited and restricted responses to requests for information	with UK government departments has been very limited. PI and other CSOs have repeatedly attempted to obtain further information but were given little additional and sometimes contradictory information.[5]	secrets or national security information), it should be made available on a confidential basis to relevant independent oversight bodies[6] (with appropriate clearance/access rights) who can evaluate their adequacy and require changes if necessary.[7] Any redactions from these documents when made publicly available must be strictly justifiable, and reviewable by an independent oversight body if necessary or challenged. Public procurement contracts should be made public (this is already a requirement in many jurisdictions). Wider PPP documentation must provide meaningful information as to the substance of the partnership, to enable understanding of the impact on the public and citizens' fundamental rights. **PPP documentation should typically include the following** (depending on the nature of the technology and services

[5] See PI and No Tech for Tyrant report, All Roads Lead to Palantir, 29 October 2020, available at https://privacyinternational.org/report/4271/all-roads-lead-palantir.

[6] Many of the safeguards recommend placing some responsibilities in an independent oversight body. Which independent oversight body will be appropriate in each case will depend on the relevant national context and the nature of the partnership involved. For example, a partnership in which the state contracts with a company for the use of communications surveillance technology will require oversight by a regulator with powers to oversee the state's investigatory powers. If the relevant technology involves mass processing of personal data, a data protection authority should be involved.

[7] For an example from Argentina of how the right of access to public information interacts with exceptions for reasons of national security, please see the submissions made by Asociación por los Derechos Civiles (ADC) to the Office of the Special Rapporteur for Freedom of Expression (RELE) of the Inter-American Commission on Human Rights (IACHR) (May 2018), available at https://adc.org.ar/wp-content/uploads/2019/06/039-acceso-a-la-informacion-publica-y-excepciones-de-seguridad-nacional-en-argentina-05-2018.pdf.

	Issue	Example(s)	Safeguard(s)
			provided, some assessments may or may not be required): • Contracts, procurement information, Memorandums of Understanding (MoUs), and any other documents providing details of the partnership • Data Sharing Agreements ('**DSA**') or Data Processing Agreements ('**DPA**') • Human Rights Impact Assessments ('**HRIA**') • Data Protection Impact Assessments ('**DPIA**') or Privacy Impact Assessments ('**PIA**') • Algorithmic Impact Assessments ('**AIA**') • Records of data processing Authorities should keep an updated **public record of surveillance technologies** used or deployed within their jurisdiction. The record should contain details and purpose of the technologies, their coverage (geography, time), and identified risks to individuals' rights and measures taken to mitigate those.
2	Commercial interests or intellectual property rights prevent disclosure of details of a technology or system	Amazon and the UK NHS: the contract obtained was largely redacted for reasons of	Companies involved in PPPs should waive commercial confidentiality and make their technologies **fully auditable** by any third party, to enable understanding of (1) what data

	Issue	Example(s)	Safeguard(s)
		Amazon's commercial interest.[8] After PI's challenge, the UK's data protection authority ordered partial disclosure.[9] Electronic voting in Paraguay: machines were made available for auditing, but neither the source code nor the hardware were open for auditing.[10]	the company and its technology have access to, (2) how the technology analyses the data and draws conclusions (including disclosure of algorithm parameters), and (3) what role the technology performs in the public authority's decision-making process. Such information should be available for public scrutiny prior to contracting. If details of the workings of a particular technology cannot be disclosed for specified and valid grounds of serious commercial harm to the company, an **independent oversight body bound by duties of confidentiality** should be granted full access to all details of the technology required to establish those details.
3	Lack of clarity about whether and what type of personal data is or will be processed	Palantir and the Cabinet Office for the Border Flow Tool: it took PI months and multiple Freedom of Information ('**FOI**') requests to understand what kind of personal data Palantir would	When personal data is envisaged to be processed as part of a PPP, any provisional or final documentation should include **details of prospective and actual data processing activities**, including at a minimum: • Categories of data subjects (note the use of wide terms such as "members of the public" tends to demonstrate

[8] Privacy International, Alexa, what is hidden behind your contract with the NHS?, 6 December 2019, available at https://privacyinternational.org/node/3298.
[9] Privacy International, Amazon Alexa/NHS contract: ICO allows partial disclosure, 27 April 2021, available at https://privacyinternational.org/news-analysis/4486/amazon-alexanhs-contract-ico-allows-partial-disclosure.
[10] TEDIC, Voto electrónico: falta de claridad de parte del TSJE a pocos días hábiles del periodo de testeo, 9 March 2020, available at https://www.tedic.org/voto-electronico-falta-de-claridad-testeo-tsje/.

	Issue	Example(s)	Safeguard(s)
		be processing – the public contract only mentioned processing of data on "members of the public".[11]	that authorities have not properly reflected on the impact of the processing) • Types of personal data, with purposes of processing for each • Sources of personal data (where the data will be obtained) and legal basis for obtaining from each of those sources This information should be published in policies directed at populations whose data will be processed.
4	Lack of clarity as to the type and level of access to data granted to the company	Palantir and the NHS: the contract contradicted the DPIA conducted with regards to Palantir's access to data.[12]	**PPP contracts should give explicit details of the company's access to data** (whether for software maintenance, customer support, audit logs or emergency purposes), and provide for corresponding safeguards to ensure security and proper handling of the data. DPIAs should assess the risks of citizens' data (in certain cases highly sensitive data) transferring to private hands and consider the suitability of associated access rights, security, retention and deletion measures.

[11] Whatdotheyknow, Record of Privacy International FOI requests to the Cabinet Office, 18 September 2020 to 3 March 2021, available at https://www.whatdotheyknow.com/request/contracts_with_palantir#incoming-1737614.
[12] Privacy International, The Corona Contracts: Public-Private Partnerships and the Need for Transparency, 26 June 2020, available at https://privacyinternational.org/long-read/3977/corona-contracts-public-private-partnerships-and-need-transparency.

	Issue	Example(s)	Safeguard(s)
5	Public access to information about PPPs is often hindered by the lack of, or unsuitability of, a legal or procedural framework for access to information (e.g. FOIA legislation)	Huawei surveillance cameras in Valenciennes: PI's numerous requests to the city of Valenciennes bounced around for months because no defined entity was designated as responsible to respond to our requests.[13]	**Legislation guaranteeing suitable access to public interest information** must exist or be passed. PPP documentation ought to be available for public consultation under such legislation. When a PPP is set up, **a person or entity within the relevant public authority should be designated responsible** for providing access to information about the deployment of a technology and related services, and their contact details should be available on any publicly accessible website notifying the deployment of the technology or within the public PPP documentation.

[13] Privacy International, Huawei in Valenciennes: a bad romance (18 November 2021), available at https://www.privacyinternational.org/long-read/4691/huawei-valenciennes-bad-romance.

II. ADEQUATE PROCUREMENT

States ought to adhere to certain formal processes for procuring and assessing the services of private companies for delivery of public duties. This is a fundamental principle of public procurement, essential for preserving the integrity of public spending and delivery of public functions. Through such procurement processes, both the state and the company ought to perform due diligence on each other to ensure they comply with their respective human rights obligations. Under the UN Guiding Principles on Business and Human Rights, companies are required to "avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved", and to "know and show" that they do not infringe on human rights through their operations or business relationships.

In the context of PPPs for the deployment of technologies with potential impact on the enjoyment of human rights, procurement processes ought to be enhanced with certain safeguards and principles. These should ensure that proper assessments of impact have been performed, and that a certain technology isn't being deployed for reasons other than its ability to fulfil the publicly approved and stated purpose (to prevent practices such as corruption, abusive lobbying, nepotism…). By requiring companies to adhere to human rights due diligence ('HRDD') obligations, states can also ensure that a technology has been properly assessed at its design and development stages, rather than solely at deployment stage. As to the post-deployment stage, the increasingly co-dependent, ongoing relationships between states and companies in the surveillance technology sphere call for similarly ongoing, accrued assessments and scrutiny throughout the partnership's lifecycle.

	Issue	Example(s)	Safeguard(s)
6	Lack of, or lack of adherence to, formal approval	Peru En Tus Manos: in Peru, a Covid-19 tracking	When awarding a contract to a company, public authorities must demonstrate adherence to **formal**

	Issue	Example(s)	Safeguard(s)
	process; and/or exceptions from such formal processes for national security issues	app, was encouraged for use by the Peruvian government despite no formal approval process having been gone through.[14] Palantir's original £1 contract with the NHS for the Covid datastore was struck without proper scrutiny and adherence to procurement processes.[15]	**public procurement processes**, and must put in place **formal documentation** governing the partnership. Any exceptions to these formal processes (for national security or other reasons) should be strictly circumscribed, and should not be used to introduce a new technology to then repurpose it for non-excepted purposes without the required approval processes or documentation. The level of scrutiny required in a procurement process should not depend on the cost of the contract, but rather on the risks raised by the intended technology deployment.
7	Lack of HRIAs or DPIAs, or those assessments not being conducted diligently	Facial recognition in Argentina: the UN SR on Privacy expressed concerns that two cities deployed facial	States, and contracting companies, should ensure that robust **human rights due diligence** processes are in place, that include into their scope the early stages of the design and development of a technology, as well as stages of deployment and use.[18] [19]

[14] Hiperderecho, Liderazgo, estrategia, y donaciones privadas de tecnología frente al Covid-19, 6 July 2020, available at https://hiperderecho.org/2020/07/liderazgo-estrategia-y-donaciones-privadas-de-tecnologia-frente-al-covid-19/. For PI coverage, see Public-Private Partnerships on Technology in Peru: A Government without horizon, 17 September 2020, available at https://privacyinternational.org/case-study/4167/public-private-partnerships-technology-peru-government-without-horizon.
[15] The Bureau of Investigative Journalism, Revealed: Data giant given 'emergency' Covid contract had been wooing NHS for months, 24 February 2021, available at https://www.thebureauinvestigates.com/stories/2021-02-24/revealed-data-giant-given-emergency-covid-contract-had-been-wooing-nhs-for-months.
[18] The UN High Commissioner for Human Rights, B-Tech Foundational Paper on Bridging Governance Gaps in the Age of Technology – Key Characteristics of the State Duty to Protect sets an "expectation that companies conduct Human Rights Due Diligence to 'know and show' how they address adverse impacts that they are, or may be, involved in including from the design and use of their products and services", available at https://www.ohchr.org/Documents/Issues/Business/B-Tech/b-tech-foundational-paper-state-duty-to-protect.pdf.
[19] The Office of the UN High Commissioner for Human Rights has developed guidance on performing corporate human rights due diligence, available at https://www.ohchr.org/EN/Issues/Business/Pages/CorporateHRDueDiligence.aspx. The OECD Due Diligence

	Issue	Example(s)	Safeguard(s)
		recognition and other surveillance software without carrying out any PIAs, and no one was able to explain their necessity proportionality.[16] Huawei in Como: the DPIA performed by the municipality didn't cover impact of facial recognition technology ('**FRT**') and didn't assess the accuracy of FRT algorithms.[17]	Details of the processes in place should be made public and available for review. When a PPP is considered, HRIAs should be performed for any general or specific deployment of a technology.[20] DPIAs should be performed for the deployment of any technology involving the processing of personal data, whether the processing is considered to be likely to result in a high risk to individuals or not.[21] Where algorithms will be used to make automated decisions, AIAs ought to be performed as well.[22]
8	DPIAs conducted as post-award compliance checkbox rather	Huawei in Como: DPIA conducted only after tender	Individual DPIAs should be conducted during the procurement process when evaluating different technologies and companies'

Guidance for Responsible Business Conduct also provides practical, operational guidance for performing human rights due diligence, available at https://www.oecd.org/investment/due-diligence-guidance-for-responsible-business-conduct.htm.

[16] Office of the UN High Commissioner for Human Rights, Statement to the media by the United Nations Special Rapporteur on the right to privacy, on the conclusion of his official visit to Argentina, 17 May 2019, available at https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24639&LangID=E).

[17] See Wired, Perché Como è diventata una delle prime città in Italia a usare il riconoscimento facciale, 9 June 2020, available at https://www.wired.it/internet/regole/2020/06/09/riconoscimento-facciale-como/. For PI coverage, see How facial recognition is spreading in Italy: the case of Como, 17 September 2020, available at https://privacyinternational.org/case-study/4166/how-facial-recognition-spreading-italy-case-como.

[20] For practical guidance on conducting HRIAs, see for example The Danish Institute for Human Rights, Human rights impact assessment guidance and toolbox, 25 August 2020, available at https://www.humanrights.dk/tools/human-rights-impact-assessment-guidance-toolbox.

[21] For practical guidance on conducting DPIAs and a sample DPIA template, see for example Information Commissioner's Office, Data protection impact assessments, available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/.

[22] For practical guidance on conducting AIAs, see for example AI Now Institute, Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability, April 2018, available at https://ainowinstitute.org/aiareport2018.pdf.

	Issue	Example(s)	Safeguard(s)
	than pre-award decision tools	awarded to A2A Smart City.[23]	ongoing services, and the results from those DPIAs should be taken into account in the decision to award a contract. **Public authorities should award a PPP contract only *after* a DPIA has been conducted, published and made available** for review by independent oversight bodies and the public for a specified amount of time.
9	Companies might be contributing to a state's mass surveillance and authoritarian practices, in exchange for the deployment of the company's technology in the country	Huawei in Uganda: Huawei has reportedly delivered surveillance training to intelligence officials, which was later used to spy on the government's opponents.[24] Gamma International found by the UK NCP to have insufficient CSR policies and human rights due diligence practices.[25]	Authorities should assess companies' human rights policies and records, and should only grant PPP contracts to companies who, as part of their human rights policies or other codes of ethics, **commit to refusing any requests by states to assist in unlawful surveillance efforts against specific groups or when there are salient human rights risks**. Previous involvement of a tendering company in human rights abuses in other countries should be a factor leading to rejection of a bid.

[23] See n 17.
[24] The Wall Street Journal, Huawei Technicians Helped African Governments Spy on Political Opponents, 15 August 2019, available at https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.
[25] UK National Contact Point, Decision in Privacy International complaint to UK NCP about Gamma International UK Ltd, 26 February 2016, available at https://www.gov.uk/government/publications/privacy-international-complaint-to-uk-ncp-about-gamma-international-uk-ltd.

	Issue	Example(s)	Safeguard(s)
10	Technologies deployed for private purposes are sometimes co-opted by public authorities for policing purposes, without required public procurement processes and safeguards	Amazon Ring has agreements with law enforcement agencies around the world granting them access to private surveillance networks.[26] Facewatch systems deployed for retail surveillance offered for use by police forces.[27] Facial recognition in London King's Cross station – FRT installed for private security purposes, later used for policing.[28]	As a principle, **public authorities should not systematically use surveillance and mass data processing systems deployed in private spaces and/or data derived from these systems**. Any use of such systems should be on an *ad hoc*, strict necessity basis following the appropriate legal framework, and accompanied by the same transparency and due process standards required for any PPP. This means, for example, that authorities should not be granted general access to such systems or data, but should rather request specific information when they need it – following the appropriate legal framework and a prescribed procedure.

[26] Privacy International, One Ring to watch them all, 25 June 2020, available at https://privacyinternational.org/long-read/3971/one-ring-watch-them-all.
[27] See PI letter to Mark Smith, CEO of Southern Co-Operative, 1 December 2020, available at https://privacyinternational.org/sites/default/files/2020-12/PI%20Letter%20to%20Co-Op%20re%20Facewatch.pdf.
[28] Privacy International, King's Cross has been watching you – and the police helped, 25 June 2020, available at https://privacyinternational.org/case-study/3973/kings-cross-has-been-watching-you-and-police-helped.

III. ACCOUNTABILITY

Accountability in human rights law "refers to the obligation of those in authority to take *responsibility* for their actions, to *answer* for them to those affected, and to be subject to some form of *enforceable* sanction if their conduct or explanation is found wanting."[29] It is a core principle that allows all other principles to be actually enforced against a "duty bearer". In that respect, states should provide ample space for civil society to be able to observe, denounce and challenge uses of technology that violate or risk violating human rights.[30]

In the context of safeguards for the deployment of PPPs, defining responsibility requires identifying obligations, duties and standards that shall be imposed upon each actor of the relationship – for example through the inclusion of references to recognised codes or tailor-made policies. The challenge is high in PPPs because the state is relying on a private actor, who is not equally bound to act in the public interest, to deliver a public function. Accountability mechanisms must therefore be particularly robust and defined *prior* to the deployment of a PPP.

	Issue	Example(s)	Safeguard(s)
11	Public authorities are often bound by specific laws or codes that uphold the state's	Thomson Reuters data sold to Immigration and Customs Enforcement (ICE), a US agency reported to have separated	When a PPP with potential impact on the enjoyment of human rights is agreed, the state's obligations to protect against human rights abuses ought to explicitly apply to the company as well. There must be some mechanism to hold the company

[29] Office of the UN High Commissioner for Human Rights, Who Will Be Accountable? Human Rights and the post-2015 Development Agenda, Summary, 2015, available at https://www.ohchr.org/Documents/Publications/WhoWillBeAccountable_summary_en.pdf.

[30] The UN High Commissioner for Human Rights B-Tech Foundational Paper on Bridging Governance Gaps in the Age of Technology – Key Characteristics of the State Duty to Protect provides that "it is imperative that States do not use the fact of their obligations to protect against human rights harms as cover to shape company practices, products and services in ways that cause or contribute to human rights violations. In this regard, all stakeholders – especially civil society and human rights organizations - have a crucial role to play in spotting these risks, calling them out and working hard to address them." Available at https://www.ohchr.org/Documents/Issues/Business/B-Tech/b-tech-foundational-paper-state-duty-to-protect.pdf.

	Issue	Example(s)	Safeguard(s)
	human rights obligations, while private companies may not always be bound by these same laws	children from their parents and detained them in horrifying conditions. Thomson Reuters was only able to point to its "Trust Principles" to demonstrate its commitment not to assist human rights violations, rather than a clear commitment to comply with human rights law while providing its services.[31]	accountable for any human rights abuses facilitated by its technology and/or services. States should therefore ensure that the companies they contract under a PPP **adopt the provisions of any relevant laws, guidelines, or codes by which the contracting public authority is bound.**[32] This should be explicitly provided for in the documentation governing the partnership.[33]
12	Technologies developed in one country supplied to another country with differing	Chinese government working with Chinese surveillance firms to develop facial recognition technology standards	States should **control exports** of surveillance technologies by assessing the potential for their use for human rights abuses. PPP documentation should append (an) **agreed-upon human rights framework(s)** which shall govern the partnership and be used throughout

[31] Sam Biddle, Thomson Reuters Defends Its Work for ICE, Providing "Identification and Location of Aliens", The Intercept, 27 June 2018, available at https://theintercept.com/2018/06/27/thomson-reuters-defends-its-work-for-ice/.

[32] In the UK, this was recommended by the Surveillance Camera Commissioner for the deployment of Live Facial Recognition by police forces, in its report Facing the Camera, Good Practice and Guidance for the Police Use of Overt Surveillance Camera Systems Incorporating Facial Recognition Technology to Locate Persons on a Watchlist, in Public Places in England & Wales, November 2020, para 4.73: "Where the third-party operation of a surveillance camera system is being conducted by a private sector contracted service provider, the police should ensure that any contract which relates to the operation of that system places a contractual obligation on the supplier to act in accordance with the provisions of the [Surveillance Camera] Code and relevant statutory provision whenever that system is being operated in partnership with, or at the request/behest of the police." Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf.

[33] UN Guiding Principle 5 provides that "As a necessary step, the relevant service contracts or enabling legislation should clarify the State's expectations that these enterprises respect human rights. States should ensure that they can effectively oversee the enterprises' activities, including through the provision of adequate independent monitoring and accountability mechanisms."

	Issue	Example(s)	Safeguard(s)
	human rights standards	considered repressive (e.g. incorporating ethnic tracking) – those same technologies are then exported.[34] Telecoms companies providing Lawful Intercept telecommunications infrastructure developed for EU standards to regimes with differing or no human rights standards.[35]	the partnership lifecycle for checking human rights compliance of the technology itself and the state's use of the technology, as well as any follow-up services provided by the company. Companies should refuse to provide their products or services to a state they are aware does not respect international human rights standards.[36]
13	Function creep – uses of a technology evolve over time without fresh new approval and oversight processes	CCTV cameras used during the Covid-19 pandemic to monitor mask wearing and social distancing in public spaces.[37]	Once a technology is approved for use, a **technology use policy** should be developed to govern the public authority's use of the technology that defines clear boundaries for the purpose and use of the technology, with an exhaustive list of authorised uses and a non-exhaustive list of prohibited uses.[38] Any use of the technology that does not comply with

[34] Avi Asher-Schapiro, China found using surveillance firms to help write ethnic-tracking specs, Reuters, 30 March 2021, available at https://www.reuters.com/article/us-china-tech-surveillance-trfn-idUSKBN2BM1EE.
[35] See for example Christopher Rhoads and Loretta Chao, Iran's Web Spying Aided By Western Technology, The Wall Street Journal, 22 June 2009, available at https://www.wsj.com/articles/SB124562668777335653.
[36] The UN Guiding Principles require companies to consider the potential use of their products as part of their human rights due diligence.
[37] See the opinion of the CNIL (French data protection authority) on the use of "intelligent video" to monitor mask wearing on public transport: CNIL, La CNIL publie son avis sur le décret relatif à l'utilisation de la vidéo intelligente pour mesurer le port du masque dans les transports, published on 12 March 2021, available at https://www.cnil.fr/fr/avis-sur-le-decret-video-intelligente-port-du-masque.
[38] This would be essential, for example, to comply with the EU's GDPR principle of "purpose limitation", which requires that personal data be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes" (Article 5(1)(b)). This principle of purpose limitation ought to be more widely applied to any use of a technology that affects individuals' enjoyment of their human rights.

	Issue	Example(s)	Safeguard(s)
			this policy should undergo a new approval process determining whether the new use would be lawful and compliant with other safeguards, and the technology use policy should be amended to reflect this new agreed use. Any new use that is wholly incompatible with the original technology deployment's purpose should be rejected.
14	Companies rely on internal "human rights councils" to demonstrate compliance with human rights frameworks, but these councils are not transparent and are sealed by confidentiality obligations	Palantir created the Palantir Council of Advisors on Privacy and Civil Liberties (PCAP) to help them "navigate the European and broader International data privacy landscapes".[39] The PCAP is advisory only, members are compensated for their time, and its discussions are confidential.[40] NSO previously pledged to engage in consultations with human rights experts on its practices, but the identity of experts and content of	If companies contracted under PPPs wish to rely on internal, private councils to demonstrate their exercise of due diligence, consideration of human rights, and legal compliance, **these councils' or audits' deliberations, conclusions and decisions should be made public.** These councils should select specific national, regional or international human rights frameworks to adhere with and disclose which frameworks were chosen for which technologies or deployments. Regular audits assessing compliance of the company's products and services with these frameworks should be conducted, and findings published.

[39] Palantir, Privacy & Civil Liberties Engineering, available at https://www.palantir.com/pcl/.
[40] Ibid.

	Issue	Example(s)	Safeguard(s)
		advice received was never made public.[41]	
15	Reliance on data-driven technologies has been shown to entrench inequalities, inaccuracies and injustice, without providing ability to question the decisions they make or lead their users to make	Palantir and vaccine distribution: a proprietary algorithm developed by Palantir has been used to distribute Covid-19 vaccines in the US, creating unexplainable disparities and inequalities in allocation of doses between states.[42]	Algorithms and other decision-making processes deployed as part of a PPP should be **open to scrutiny and challenge** – by being auditable (as required by safeguard 21 below). The ability to audit technologies is particularly essential in order to provide adequate oversight and redress (for example, if a technology has led to a result that is later challenged in court or used as evidence, the proper administration of justice requires the technology to be entirely auditable). As part of the procurement process, the assessment of different systems should **compare their levels of discriminatory bias**. If discriminatory bias is identified, it should be rectified, and if it cannot be rectified, the technology should not be deployed.

[41] See Letter from Rights Groups to NSO Group, NSO Group continues to fail in human rights compliance, 27 April 2021, available at https://www.accessnow.org/cms/assets/uploads/2021/04/Rights-groups_NSO-Group-continues-to-fail-in-human-rights-compliance_27-April-2021.pdf.
[42] The New York Times, Where Do Vaccine Doses Go, and Who Gets Them? The Algorithms Decide, 7 February 2021, available at https://www.nytimes.com/2021/02/07/technology/vaccine-algorithms.html?referringSource=articleShare.

IV. LEGALITY, NECESSITY AND PROPORTIONALITY

The use of a technology or system to deliver public functions can only ever be legitimate if it is "legal", in the sense of falling under an appropriate legal framework that authorises such technology to be used for such purposes. This is the principle of legality, a fundamental principle of international human rights law that requires any interference with human rights to be "prescribed by law".[43] In addition, international human rights law requires that any interference with the right to privacy must be necessary and proportionate.[44] Any technology deployed by the state that has an impact on its citizens' privacy must therefore demonstrate in "specific and individualized fashion the precise nature of the threat" that it seeks to address.[45] In addition, the principle of proportionality requires that the interference with privacy be both "in proportion to the aim and the least intrusive option available."[46]

In the context of PPPs, assessments of legality, necessity and proportionality should be performed *prior* to any contracting with private companies, as well as *during* the contracting relationship before any individual deployment of the technology.

	Issue	Example(s)	Safeguard(s)
16	Privacy-invasive technologies are deployed without	Mobile Phone Extraction ('**MPE**') technology has	When considering the need for, and the deployment of a technology to address a public need or fulfil a

[43] See European Convention on Human Rights Articles 8-11, International Covenant on Civil and Political Rights Articles 12, and 17-22, and Inter-American Convention on Human Rights Articles 11-13, 15, and 16.
[44] See UN Human Rights Committee, *Toonen v Australia*, Comm. No. 488/1992, UN Doc CCPR/C/50/D/488/1992, 31 March 1994, para 8.3 ("[A]ny interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case."); Office of the UN High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37, 30 June 2014) ("OHCR Report on the Right to Privacy in the Digital Age"), para 23 ("These authoritative sources [U.N. Human Rights Committee General Comments 16, 27, 29, 31, and 34 and the Siracusa Principles] point to the overarching principles of legality, necessity and proportionality […]").
[45] UN Human Rights Committee, General Comment No. 34 (Article 19 ICCPR), 12 September 2011, para 35.
[46] OHCR Report on the Right to Privacy in the Digital Age (n 44), para 23.

	Issue	Example(s)	Safeguard(s)
	appropriate legal framework authorising and governing their use	been deployed by police forces in the UK for years without a proper legal framework.[47] Huawei in Valenciennes: Huawei deployed surveillance cameras equipped with facial recognition technology in the city of Valenciennes, while FRT is not legally authorised in France.[48]	public function, the state must consider whether **an appropriate legal framework authorises the use of such technology for the intended purpose**. The technology should not be experimented with nor deployed before appropriate statutory (not secondary) legislation is passed. Legislation will be appropriate if it authorises the use of the specific technology, by the specific authorities, for the specific purpose – general legislation (e.g. granting blanket powers or complete discretion to law enforcement authorities) will not be sufficient. A proper legal framework must also contain specific policies and guidance governing the use of the technology (such as the technology use policy put forward in safeguard 13).
17	Technologies deployed through PPPs are not always necessary to achieve stated goals	Huawei in Belgrade: the DPIA did not establish that the use of smart video surveillance was necessary for public safety as it overestimated its positive effects on crime reduction.[49]	As part of an adequate DPIA and/or HRIA, a **necessity assessment** must be conducted to clearly demonstrate that recourse to a particular technology or data analytics system is necessary to achieve defined goals, rather than a mere advantage. As part of this assessment, any projected positive effects of a technology should be assessed through a collection of

[47] Privacy International, Digital Stop and Search: how the UK police can secretly download everything from your mobile phone, March 2018, available at https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf.
[48] Privacy International, Huawei in Valenciennes: a bad romance (18 November 2021), available at https://www.privacyinternational.org/long-read/4691/huawei-valenciennes-bad-romance.
[49] SHARE, "Thousands of Cameras" - a citizen response to mass biometric surveillance, 25 June 2020, available at https://privacyinternational.org/case-study/3967/thousands-cameras-citizen-response-mass-biometric-surveillance.

	Issue	Example(s)	Safeguard(s)
			independent evidence sources and comparative practices.
18	Technologies deployed through PPPs often have an impact on human rights disproportionate to their intended purpose	Huawei in Como: the need for a facial recognition system was justified in official documentation by an isolated incident that occurred years before.[50]	As part of an adequate DPIA and/or HRIA, a **proportionality assessment** must be conducted to measure the adverse impact on citizens' rights and freedoms and demonstrate that it is justified by a corresponding positive impact on citizens' welfare. These assessments should take into account the potential chilling effects on other rights such as the rights to freedom of expression and freedom of assembly, which can be affected by surveillance and data processing systems in ways that can be difficult to anticipate and measure.

[50] See Wired and Privacy International (n 17).

V. OVERSIGHT

The UN Guiding Principles on Business and Human Rights require that states exercise "adequate oversight in order to meet their international human rights obligations when they contract with, or legislate for, business enterprises to provide services that may impact upon the enjoyment of human rights."[51]

Continuing oversight of the deployment and results of a technology is essential to ensure that accountability mechanisms are properly used and work to constrain the use of the technology to its stated purpose, detect abuses or resulting harm, and require redress. The UN Special Rapporteur on Counter-Terrorism and Human Rights has explained that "[s]urveillance systems require effective oversight to minimize harms and abuses." The Special Rapporteur recommended that "[s]trong independent oversight mandates […] be established to review policies and practices, in order to ensure that there is strong oversight of the use of intrusive surveillance techniques and the processing of personal information."[52] The safeguards in this section therefore recommend concrete ways of establishing relevant oversight mechanisms, that address the potential harms caused by the deployment of private technologies on affected individuals and communities.

	Issue	Example(s)	Safeguard(s)
19	No independent entity responsible for overseeing the partnership and its obligations to the public	MPE in the UK: the use of mobile phone extraction ('**MPE**') technology by police forces in the UK went on for years in ways the ICO later	When a new PPP is deployed, **establish or designate an independent oversight body** (depending on the technology and authority concerned, this could be the country's data protection authority if one exists, or an authority responsible for overseeing

[51] UN Guiding Principle 5.
[52] 2009 Report of the UN Special Rapporteur on Counter Terrorism (n 4), para 62.

	Issue	Example(s)	Safeguard(s)
		found inappropriate and unlawful.[53]	investigatory powers) responsible for (1) reviewing, approving or rejecting new proposals for use of the technology or system deployed as part of the PPP, (2) undertaking regular audits of the technology deployment including public consultations on the impact of a technology on the rights of civilians and the achievement of its intended objective(s), and (3) receiving grievances and mediating those between the public and the entities using the technology.[54] This independent oversight body should be given appropriate resources (human and financial) to be able to perform its duties.
20	Lack of consultation of communities and civilians affected by the deployment of technologies	Amazon Ring and police forces: no consultations of communities prior to co-opting Ring's private security cameras by law enforcement.[55]	When a technology is likely to affect certain communities in a disproportionate way, **institute a "civilian control board"** composed of individuals directly affected by the technology, in particular those at risk of discrimination. This control board should be consulted prior to deployment of the technology, seek consent of the affected population, and be tasked with receiving and voicing grievances as to the impact of the technology on individuals'

[53] See recommendations regarding oversight in Information Commissioner's Office (ICO), Mobile phone data extraction by police forces in England and Wales – Investigative Report, June 2020, available at https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf.
[54] In the UK, for example, the Surveillance Camera Commissioner recommends that "where police forces are considering operating LFR [Live Facial Recognition] they should develop mechanisms which provide for meaningful and independent 'ethical oversight' of their decision making and operational conduct. Such considerations should be applied as part of the initial police planning processes and be established before any operational activity commences." (Facing the Camera, n 32, para 2.26).
[55] See Privacy International (n 26).

	Issue	Example(s)	Safeguard(s)
			rights throughout the deployment's lifecycle.
21	Lack of ongoing impact assessments	Police forces in the US do not record questionable or negative results of facial recognition technology ('**FRT**'), producing a one-sided, entirely positive view of FRT.[56]	Throughout the lifecycle of a technology's deployment, public authorities ought to record indicators of performance of the technology such as successes, failures, accuracy levels, purpose and outcome.[57] Through an independent oversight body, and in collaboration with a civilian control board, they should carry out **regular audits** of the technology and **updates to relevant HRIAs**. These audits should include **regular consultations** with groups and individuals affected by the technology (in particular those at risk of discrimination) and with CSOs, to evaluate the ongoing or potential impacts of the technology in a holistic way. A **"retrospective" audit** should also be performed after the contracting relationship has ended, as the impacts of a technology on human rights can sometimes be delayed. Conclusions of such audit should be published and inform the assessments of all future PPPs.

[56] Jennifer Valentino-DeVries, How the Police Use Facial Recognition, and Where It Falls Short, 12 January 2020, The New York Times, available at https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html.
[57] Similar types of performance indicators were recommended by the Surveillance Camera Commissioner to be developed by the UK's National Police Chief's Council to assess the impact of LFR operations (Facing the Camera, n 32, para 6.10).

VI. REDRESS

Many things can go wrong with the deployment of a private technology for performing state functions, potentially leading to severe impacts on individuals' human rights. If such things happen, international human rights law provides that states have an obligation to ensure an "effective remedy" for individuals whose rights they have violated.[58] States have a legal obligation to provide effective remedies for "business-related human rights harms, including human rights harms associated with the development and use of digital technologies by companies".[59]

In the context of surveillance or processing of personal data, the secrecy around technologies used renders such redress particularly difficult to obtain. While recognising that "advance or concurrent notification might jeopardize the effectiveness of the surveillance", the UN Special Rapporteur on Freedom of Expression has emphasized that "individuals should nevertheless be notified once surveillance has been completed and have the possibility to seek redress in respect of the use of communications surveillance measures in their aftermath".[60]

In the context of PPPs, the common lack of information due to confidentiality restrictions can affect redress. Redress needs to be justified, designed and assigned in a way that corresponds to the way a technology functions and is

[58] See Universal Declaration of Human Rights, UN General Assembly Resolution 217 (III) A, 10 Dec. 1948, Art. 8 ("Everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted him by the constitution or by law"); Art. 2(3), International Covenant on Civil and Political Rights ("Each State Party to the present Covenant undertakes: (a) To ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity"); Art. 25, ACHR ("1. Everyone has the right to simple and prompt recourse, or any other effective recourse, to a competent court or tribunal for protection against acts that violate his fundamental rights recognized by the constitution or laws of the state concerned or by this Convention, even though such violation may have been committed by persons acting in the course of their official duties"); Article 13, ECHR ("Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."). See further UN General Assembly Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law, UNGA resolution 60/147, 16 December 2005.

[59] UN Human Rights Office of the High Commissioner, B-Tech Foundational Paper, Access to remedy and the technology sector: basic concepts and principles. Citing UN Guiding Principle 25, available at https://www.ohchr.org/Documents/Issues/Business/B-Tech/access-to-remedy-concepts-and-principles.pdf.

[60] Report of the U.N. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc. A/HRC/23/40, 17 April 2013, para 82, available at https://undocs.org/A/HRC/23/40.

used – hence the need for other principles to have been properly upheld, in particular transparency, accountability and oversight.

Equally, states ought to have recourse against companies that violate any conditions of their agreement with the state or that ought to be held responsible for facilitating abuses of human rights. This is essential for states to be able to uphold their obligations towards citizens when fault is attributable in whole or in part to the company they contract with.

	Issue	Example(s)	Safeguard(s)
22	Lack of avenues for redress when a technology is abused	NSO malware used to target lawyers of victims in Mexico – once discovered, NSO did not cooperate with efforts to obtain accountability and redress.[61]	Having recourse to courts or other senior judicial systems is often not a viable option for individuals affected by isolated uses of a technology, especially considering that abuse can be difficult to establish through traditional justice mechanisms. The technology use policy recommended by safeguard 13 should include **redress provisions** by pointing to existing, or establishing new, mechanisms and entities for complaints handling and enforcement of sanctions for violations of the policy (including pointing to an appropriate independent oversight body able to investigate and provide redress). These redress mechanisms and responsible entities should be suited to the nature of the technology, its intended purpose and identified impacts. They should assign responsibilities and redress obligations to both the state and the

[61] Citizen Lab, Reckless IV – Lawyers for Murdered Mexican Women's Families Targeted with NSO Spyware, 2 August 2017, available at https://citizenlab.ca/2017/08/lawyers-murdered-women-nso-group/.

	Issue	Example(s)	Safeguard(s)
			company involved, and ought to adhere to the eight "effectiveness criteria" set out in UN Guiding Principle 31. That said, any redress provisions must not bar access to courts or other established judicial mechanisms. They must strike the right balance between accessibility of redress and compliance with the rule of law. The state should also ensure that the company they contract with has a grievance mechanism in place,[62] through which potential adverse human rights impacts can be flagged and remedied early.
23	PPP contracts tend to lock public authorities and companies in the partnership through onerous switching or termination clauses	UK Border Agency sued by Raytheon Systems Limited for wrongful termination of immigration computer system provision contract.[63] Palantir and the NYPD: at the end of the contract, Palantir refused to produce the analysis generated by	PPP contracts should include **termination clauses** allowing (1) the company to terminate the contract should it become aware that its technology has been used or is intended to be used for activities which do not comply with the governing human rights framework, and (2) the state to terminate the contract should it become aware that any of the company's products has been used for human rights abuses by other states (regardless of whether the product in question is the one contracted for), or if it becomes apparent that certain terms of the

[62] This is required by UN Guiding Principle 29.
[63] See Computer Weekly, UK government pays £150m to Raytheon to settle e-Borders dispute, 27 March 2015, available at https://www.computerweekly.com/news/4500243244/UK-government-pays-150m-to-Raytheon-to-settle-e-Borders-dispute.

	Issue	Example(s)	Safeguard(s)
		Palantir's software for it to be transferred to a new non-Palantir system.[64]	contract prevent the state from acting in the public interest. PPP contracts should also include strict **interoperability and transferability clauses**. Interoperability and transferability are essential in the realm of public procurement, as a state is bound to procure services that comply with certain requirements and to do so in a prescribed way. If a company previously contracted with changes the way its service(s) work, or its policies, making them incompatible with the state's obligations, the state should be entirely free to exit this partnership and enter another, without any hoarding of data or information by the company nor any "punitive" or otherwise undue costs of switching, which put pressure on public funds.

[64] See Buzzfeed News, There's A Fight Brewing Between The NYPD And Silicon Valley's Palantir, 28 June 2018, available at https://www.buzzfeednews.com/article/williamalden/theres-a-fight-brewing-between-the-nypd-and-silicon-valley.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org