

CHALLENGING PUBLIC PRIVATE SURVEILLANCE PARTNERSHIPS: A Handbook for Civil Society

June 2022

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.



Open access. Some rights reserved.

Privacy International wants to encourage the circulation of its work as widely as possible while retaining the copyright. Privacy International has an open access policy which enables anyone to access its content online without charge. Anyone can download, save, perform or distribute this work in any format, including translation, without written permission. This is subject to the terms of the Creative Commons Licence Deed: Attribution-Non-Commercial-No Derivative Works 2.0 UK: England & Wales. Its main conditions are:

- You are free to copy, distribute, display and perform the work;
- You must give the original author ('Privacy International') credit;
- You may not use this work for commercial purposes;

You are welcome to ask Privacy International for permission to use this work for purposes other than those covered by the licence.

Privacy International is grateful to Creative Commons for its work and its approach to copyright. For more information please go to www.creativecommons.org.

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

ACKNOWLEDGMENTS IV

INTRODUCTION 2

1. RISK ASSESSMENT 4

A. RISKS TO CONSIDER 4

B. SUGGESTED MITIGATIONS 5

2. UNCOVERING INFORMATION 6

A. USING ACCESS TO INFORMATION LAWS 6

B. OTHER RESOURCES 8

i. Open source intelligence 8

ii. Procurement data 10

iii. Stakeholders as sources of information 11

C. *CHECKLIST – UNCOVERING INFORMATION* 13

3. UNVEILING AND UNDERSTANDING THE UNDERLYING TECHNOLOGY 14

A. IDENTIFYING THE BLOCKS OF THE TECHNOLOGY AT STAKE 14

i. Data collection/capture system (hardware/software) 15

ii. Data transmission system (hardware/software) 16

iii. Data storage system (hardware/software) 17

iv. Data processing system (software) 19

v. A note about prioritising blocks of technology 20

B. ASSESSING NOVELTY/INNOVATIVENESS 21

i. Entirely new technology 21

ii. New features/capabilities 22
iii. A note about technical protocols and standards 23
C. UNDERSTANDING HOW THE TECHNOLOGY AT STAKE FUNCTIONS 25
i. Added literature review 25
ii. Using and testing existing alternatives 26
iii. Questioning experts 27
D. *CHECKLIST – UNDERSTANDING THE TECHNOLOGY* 29
4. GOVERNANCE CONCERNS 30
A. UN GUIDING PRINCIPLES ON BUSINESS AND HUMAN RIGHTS 30
i. UN Guiding Principles as a standard of conduct for companies 31
ii. Technology companies and UN Guiding Principles 31
iii. UN Guiding Principles as the global authoritative standard 32
B. DATA PROTECTION/PRIVACY CONCERNS 34
i. Data sources 35
ii. Lawfulness and fairness 35
iii. Transparency and the right to be informed 37
iv. Data storage and access controls 38
v. International data transfers 39
C. ACCOUNTABILITY AND OVERSIGHT 40
D. *CHECKLIST – GOVERNANCE* 43
ANNEX: THE HANDBOOK'S CHECKLISTS 46

ACKNOWLEDGEMENTS

With thanks to our partner organisations: ADC, TEDIC, and another organisation that wishes to remain anonymous who contributed to this handbook.

- The Association of Technology, Education, Development, Research and Communication (TEDIC) is a Paraguayan NGO founded in 2012 that develops open civic technology and defends digital rights for a free culture on the internet.
- Asociación por los Derechos Civiles (ADC) is a civil society organization based in Argentina that, since its foundation in 1995, works to defend and promote of civil and human rights in Argentina and Latin America.

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 collaborations 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 requires more scrutiny than ever 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.

Civil society has the power to expose the risks and issues that emerge from these partnerships through investigation and public reporting. But identifying concrete risks and potential human rights abuses is not an easy task for anyone as it requires a multilevel understand of the tech, law and governance involved. Building on our own investigative work and on the expertise of our partners, Privacy International has designed a handbook for civil society organisations,

non-governmental organisations, academics and individuals to navigate these partnerships, providing keys to obtain crucial information, understand the technology at stake and identify privacy and governance concerns.

To support anyone trying to find out more about a public private surveillance partnership and identify key risks and issues, this handbook is divided in to four main sections: the first section looks at how to review risks involved, the second section focuses on gathering key information related to the partnership through a variety of means; the third section delves into the technology at play in the partnership, taking a top to bottom approach starting with ways to broadly define what the technology is and ending with methods to understand how the technology actually functions; the fourth section looks into governance concerns and safeguards, including international best practice, data protection issues, and relevant safeguards.

The checklists provided at the end of this handbook can be used as an overview of key things to investigate, and to help you keep track of your work.

This handbook is intended to help you:

- Investigate a public-private partnership, find out relevant information
- Ask the right questions to the partners involved (private and public)
- Identify concerns related to the technology involved and the governance of the partnership

We have separately developed a set of safeguards for public-private surveillance partnerships, that you can use for advocacy ideas once you have identified concerns through this handbook.

1. RISK ASSESSMENT

Investigating a public-private partnership comes with a number of legal, technical, and human risks that must be assessed before undertaking any action. These risks change with your research framework and the broader context within which the partnership operates. We suggest you identify and assess the risks related to your investigation project before anything else. To assist you with this task you may refer to the non-exhaustive lists below.

A. RISKS TO CONSIDER

- Defamation: The law of defamation protects a person's reputation against unjustified interference. You may get sued for defamation by a private actor you make allegations against. Defamation laws differ between jurisdictions and the burden of proof might be entirely on you.
- Unlawful obtention of information: Depending on your jurisdiction, certain types of investigations might be in contravention of the law (such as publishing leaked information or hacking).
- Intellectual Property (IP): Trade secrets and copyright are two examples of IP law that you might break while carrying out your investigation.
- Risks for people (staff, source, partners…): Any activity that can put at risk the life of someone involved should not be undertaken, unless there are specific actions to be taken to mitigate the risks. Risks may include among others: physical harm, psychological harm, social harm, economic harm, and legal harm.
- Damage to reputation: Risks for your organisation's objectivity, impartiality or credibility. Risks may include: inaccurate facts, insufficiently backed statements, and exploitation of social media monitoring (SOCMINT) and other open sources (OSINT) without consideration for privacy, etc.

B. SUGGESTED MITIGATIONS

Below are some suggested mitigations for these risks. They are not exhaustive, and may not, alone, be adequate to successfully mitigate all these risks.

- Strong research methodology: Citing sources, evaluating quality of sources, taking photos and videos, use of adequate language.
- Corroboration of information: Corroborating multiple sources and testimonies to ensure validity of the information.
- Redaction and cleaning of documents: Redacting personal data and stripping documents of metadata.
- Preparation before public speaking or media interviews to adopt adequate language.
- Keep original sources and store them securely.
- Consider the safety of people (consent, anonymity and more) before undertaking any action.

2. UNCOVERING INFORMATION

Obtaining adequate information about a public-private partnership is often difficult, especially when sensitive areas of government are involved, such as intelligence and law enforcement. Information about such activities is often purposefully withheld from the public and guarded by excessive laws and punishments.

But if it is safe to access them, there are many methods and resources out there which can help. Many of these sources are already readily available online, while others require desk work and engaging people who might be able to help.

Not all of these are readily accessible or safe to access from everywhere: governments around the world are known to punish activists, journalists, and others for exposing or even seeking information about such contracts, so risk assessments and mitigations are required.

A. USING ACCESS TO INFORMATION LAWS

A request under freedom of information (FOI) or other access to information laws (such as right to information laws (RTI)) is a formal request you make to a public body (your local, regional, or municipal authorities, the police, a ministry etc.) in order to access information that the public is entitled to know about. You may be trying to obtain a contract the partners have signed, some correspondence (emails or letters) between the partners, some official statistics, or simply an answer to a question, or even other documents such as a presentation given to the public authority by a company. Some laws specify what you can and cannot request – Uganda for example requires you to request specific documents, meaning you can't ask questions.

Information obtained under such requests are an invaluable tool for journalists, activists, and the public: the more information that is available to the public, the better informed we are as a society and the easier it is to demand changes.

However, while such laws typically promise much, and while more than 90 countries have laws which require officials to provide public records, in practice getting them to do so is not so simple.

When submitting such requests, it is important to remember a few key recommendations:

- Check what you're looking for is not already out there
- Know who you are sending to
- Keep it focused!
- Speak their language
- Be prepared to be patient!

Privacy International has a guide that outlines some of the lessons we have learned from filing such requests around the world.

The Global Investigative Journalism Network has an excellent list of FOI resources available in many countries across every continent. We really recommend you take a look at it – many of the FOI guides we love are in that repository.

It's important to remember that useful public records may exist in other jurisdictions. In cases where a company is headquartered in one country but is operating in another, it may be worth submitting requests in either jurisdiction. For example, journalists have been able to find out more information about the provision of surveillance technology to North Macedonia by submitting requests to authorities in the UK which oversaw the authorisation of the export. Although some countries (e.g. India) only allow requests from citizens.

What our partners say:

Access to information laws can be useful tools but can also be disappointing. You should keep in mind that your request might be left unanswered and plan accordingly for other ways to obtain information.

Some of our partners told us they found information requests most useful for confirming things they already found from other sources, others found them more useful from a public communications perspective or to learn more from the reason the request was rejected.

B. OTHER SOURCES

i. Open Source Intelligence

When trying to find out more information on public-private partnerships, there are a lot of publicly accessible sources that can provide additional information – gathering and using this information is sometimes referred to as Open Source Intelligence (OSINT).

Organisations such as Bellingcat have used OSINT extensively to uncover governments' unlawful practices and human rights abuses - including on some of the most well-protected and secretive government agencies around the world.

Access to useful information however depends on a number of factors, including the country in which the partnership is based, the type of company involved, and the type of technology or service it is providing.

There are multiple resources online and across publications that provide information on OSINT gathering, including:

- Bellingcat
- i-intelligence
- The Tow Center for Digital Journalism
- the OSINT Framework

Many techniques however raise important security, ethical and legal questions that must be considered. The Human Rights Center at Berkeley School of Law and the UN Office of the High Commissioner for Human Rights have developed a guide on the use of OSINT in investigating violations of international criminal, human rights and humanitarian law, which provides some guidance on such considerations.

For example, as the guide notes, it might be illegal in some jurisdictions to misrepresent your identity on social media. Even if it is not, it may still be a breach of the terms of service of the social media company, and if a false identity is used to access or solicit otherwise inaccessible information from an individual or group, it may violate ethical principles or the law.

Open sources of data for accessing information on public-private partnerships include:

- Company websites, which may outline their products and sometimes even publish lists of customers.
- Company filings to regulators, which often outline important information like their business activities, structure, and revenue. Researchers have been able to make detailed analyses of companies' corporate structures using such information. Such information is available on platforms such as OpenCorporates.
- Job advertisements placed on commonly accessible recruitment and social media sites like LinkedIn. These often provide clues or details as to what business activities a company is engaged in and where, and what innovations are in the pipeline: for example, a UK journalist was able to access information on a secretive government "super database" using job posting information.
- Shipping and trade data, commonly made available by some governments and companies. For example, Indian authorities publish shipping data about imports and exports, some of which are then accessible on commercial websites. This can be used to identify certain exports: for example, Forensic News identified that an Israeli spyware company had shipped equipment to Uzbekistan's secret police using shipping data.

- Government aid transparency data. This can often outline instances where government authorities have provided equipment, financing or training to counterparts around the world and therefore provide information about what software or equipment they have access to. For example, using US aid data, it's possible to map surveillance companies whose products have been provided to governments in Central America.
- Social media networks, including for example professional social networks such as LinkedIn. This is a common source for journalists and can be used to identify certain information regarding individuals and companies but must be used ethically and legally (see above).

ii. Procurement Data

Government procurement data is one of the best open sources for finding information about public-private partnerships. Centralised government procurement sites are available in addition to tender documentation on agencies' dedicated websites, though in-depth details are often restricted.

Publicly accessible information on tenders - notices which specify that a government authority is seeking to procure a service or product from the private sector - can provide valuable insights. Often the tender will only provide general information, but it can nevertheless serve as a basis for further research, for example through the submission of a Freedom of Information Access (FOIA) request.

For example in the UK, a centralised, publicly-available, and searchable platform exists that allows anyone to search for tenders by government agencies (though in practice many details are withheld on national security grounds).

Similarly, the US, the EU, Russia, and other countries around the world publish tenders on government websites.

Using such government procurement documents in the run up to the Sochi Winter Olympics in 2014, for example, journalists were able to establish and map

how the Russian security services were planning to monitor phone and internet communications throughout the games.

After spotting a tender from Frontex (the EU's border agency) looking for a surveillance company to track people on social media, Privacy International responded with detailed questions about the scheme's legality. Two days later Frontex cancelled the tender.

Sometimes, these same sites or similar ones will also provide information on which contracts have been awarded to which company. For example, in the US the federal procurement website provides data on which companies have been awarded contracts. These are regularly used by journalists to access and report on such information, although details are again usually minimal. Tech Inquiry provide a searchable platform through which contracts reported by Australian, Canadian, US, and UK authorities can be searched.

Privacy International also have a guide aimed at researchers and journalists on some available open sources which can be used to identify surveillance exports.

A free online course to learn more about privacy and researching surveillance technology developed by Privacy International is available on Advocacy Assembly.

iii. Stakeholders as sources of information

In addition to desk research and formal requests, getting in touch with individuals that are involved in or might know about a public-private partnership can give access to information or perspectives that are crucial to your work.

Academics, members of the government, people working in similar private companies can all be useful sources of information for your work when approached properly and with adequate research practices in place (such as anonymisation).

Journalists that have covered the partnership you are looking into might also have had access to important sources and be willing to share additional details with you when contacted directly.

Similarly, there might be other organisations or groups looking into the same partnership. Try to coordinate with these groups to share information and potentially build stronger advocacy later.

When approaching people involved directly with the partnership at stake, you should ensure that they feel safe and that you understand their position. Being accommodating and avoiding accusation are key to obtaining important information. You should always be sensitive to concerns that they may have. Under all circumstances, it is essential to discuss and agree in advance on the conditions of this exchange of information. Always seek help and advice if you are not sure how to handle a source.

Disclaimer: Before undertaking any interview make sure you have done a proper risk assessment and seriously considered risks to your organisation, as well as to the people you are talking to. You should ensure you can provide an adequate level of privacy and security, and the you understand the legal implications, before engaging with people who may be putting themselves at risk by sharing information.

What our partners say:

If the PPP you are looking at is targeting a specific region or area, looking into local newspapers, Facebook groups, and local organisations can reveal important information. These groups might have access to information that isn't widely known or might be in contact with key people involved in the partnership.

ADC, in Argentina, once obtained key information by looking at a Facebook group of locals trying to rally against a project happening in their area.

Our anonymous partner found that interviewing stakeholders who've recently left an organisation can help you to understand where, for example, policies aren't an accurate reflection of reality.

C. CHECKLIST – UNCOVERING INFORMATION

To help you in in your research you might want to use this checklist:

- ☐ Have you considered the ethical, legal and security implications of accessing and/or sharing the information you are looking for?
- ☐ Have you considered possible risks and mitigations unique to your context and circumstances?
- ☐ Is the information you are looking for already easily accessible in the public domain?
- ☐ Does the jurisdiction you are interested in have freedom of information or access to documents law that you could use?
- ☐ Are there relevant guides or courses available on how to conduct certain open source research techniques that might help find what you are looking for?
- ☐ Are there any open sources you could access in your country to find the information?
- ☐ Are there any open sources you could access that are located abroad to find the information?
- ☐ Are there any individuals or organisations out there who might be able to help you find the information that you can engage securely?
- ☐ Have your sources given you appropriate and properly informed consent?
- ☐ Have you considered how to handle the information you receive from your sources?
    - ☐ Where will you save the information?
    - ☐ Do you need to anonymise it? Pseudonymise it?
    - ☐ Do you need to redact information? How will you do that thoroughly?
    - ☐ Are there any contextual details in the information that might point towards your source or anyone else?

3. UNVEILING AND UNDERSTANDING THE UNDERLYING TECHNOLOGY

Technologies at the heart of a public-private partnership can be surrounded by secrecy and opacity making it hard for external actors to assess the risks. From buzzwords to obscure technical terminology, getting a real sense of what the technology at stake is and what it actually does isn't an easy job. This section is designed to guide you in finding more information about the technology, understanding it, and identifying potential flaws.

A. IDENTIFYING THE BLOCKS OF THE TECHNOLOGY AT STAKE

The first step when looking at technology is to find basic information about it - to define and categorise it. Looking at the Wikipedia page of a given technology is often a good starting point and will help you clarify what is implied within a technology (for example for Facial recognition). This is particularly useful when there is no specific technology that is mentioned in the partnership or when you are looking at a tender. You might also want to check the company's marketing materials to get a sense of what they specialise in and the type of product they offer.

Sometimes a partnership will involve more than one technology, sometimes across more multiple contracts and/or partnerships – such as an ID system that may require a fingerprint scanner and a database, that may be supplied by different companies.

Getting a broad sense of what you are looking at is a simple but very important step to be able to move forward and identify risks. **Your goal is to be able to**

give a broad but accurate high-level definition of what technology is at stake in the partnership.

Examples of high-level descriptions of a technology:

- Facial recognition system – A system capable of matching faces identified in a given image or video with a dataset of previously identified human faces.
- Ankle tracking bracelet – A physical bracelet attached to someone's limb capable of recording and transmitting geolocation or proximity with a base tag.
- Unmanned Aerial Vehicle – An autonomous or remotely controlled aerial vehicle capable of taking predefined actions and collecting, processing and transmitting environmental data such as images, temperatures, and sounds.

With this first step done, you will rapidly realise that technologies will usually rely on multiple physical and logical elements to function. Breaking it down and identifying each layer is therefore the next logical step in understanding how the technology functions and what are the potential points of failure. For example, a facial recognition system captures, transmits, stores, and processes data. Different elements play a key role in each of these steps.

These layers can be hardware, software, or a combination of both. The collection of technologies behind a simple term such as "a database" might be complex. The more thorough you are in dividing it into blocks the better an understanding you'll have of what's at stake and its potential risks.

Using a data-centered approach, the different elements composing the technology will usually fit into one of the following **four** categories:

i. Data collection/capture system (hardware/software)

Data collection amounts to capturing information. This could consist in a camera taking a picture, a sensor capturing information like temperature, software registering an action such as a click on a button or a Mobile Phone Extraction device grabbing data from a phone. Data collection systems can be physical

devices, such as a satellite equipped with sensors, or virtual, such as an app or a web scraper (a piece of code that crawls the internet to collect data).

Why it matters

Understanding what part of the technology is in charge of the data collection enables you to understand what data is collected (images, sound, user entered data), where it comes from (sensors, user interactions) and under what circumstances it is collected (with or without the person knowing, how often, etc.). This enables you to identify potential issues regarding the legality of the collection or the accuracy of the data collected.

Examples of a data collection system:

- A network of cameras in a city
- A website to register for a public event
- A satellite with a variety of sensors taking photos of a given area
- A fingerprint reading machine at the airport

Potential risks in data collection

Data collected can be incorrect, sensors can be rigged, data can be collected without consent or other legal basis, the physical sensors can be degraded over time, the logic or set of instructions (for a software) can be biased or incorrect, the device can be vulnerable to attack (overloaded, provided with incorrect information etc.).

ii. Data transmission system (hardware/software)

Once the data is collected it might be transmitted to another system for storage or processing, for example a server. Transmissions will usually happen through existing solutions with well-defined protocols such as the internet protocol suite (TCP/IP) for communication between devices on the same network (like two servers connected to the internet or a smart camera and a computer connected

to a private network) but might sometimes be the innovation at stake (e.g. the New IP proposal made by China at the International Telecommunication Union (ITU) or 5G New Radio, the global standard for the air interface of 5G networks).

Why it matters

Understanding if and how data is transmitted enables you to identify potential security risks (if transmission isn't secured, for example using an unsecured Wi-Fi network), existing concerns (if a protocol/network is outdated and has known vulnerabilities as 2G) or technical requirements (e.g. distance at which Bluetooth can function to reliably transmit data) to better assess suitability in the given context.

Examples of data transmission systems:

- The internet protocol suite (TCP/IP, the protocol on which is build most of the internet technologies)
- The Global System for Mobile Communications (GSM)
- Bluetooth
- Satellite communications via High frequency radio waves

Potential risks in data transmission

Technology can be insecure (poor or low level of encryption, known vulnerabilities and so on), data can be degraded/lost in transit, data can be intercepted/tampered with, the system can pose health threats, the system can be interrupted by external factors (Denial of Service attack on a network, destruction of emitter/receiver and more).

Note: To learn more about protocols, standards, standardisation bodies, see "A note about technical protocol and standards" at the end of this chapter.

iii. Data storage system (hardware/software)

After capture and transmission of the data, it might be stored somewhere for processing or archiving purposes. Storage systems will usually rely on some form of storage device such as a hard drive, an SD card, a USB stick, often as part of a bigger system if regular access is required (laptop, server…). The variety of software in charge of storing and accessing this data is massive, from database software such as MySQL to blockchain-based systems that offer immutability.

Why it matters

Identifying where and how the data is stored allows you to better understand the implications (the software/method used might be prone to security vulnerabilities or frequently targeted by attacks such as an ElasticSearch database or similar Bucket product), **retention** (the system might only allow for data to be stored for a certain amount of time or, on the contrary, store data indefinitely such as a blockchain system), **access-control** (a system with too-loose permission can allow unauthorised access) and **durability** (the expected lifetime of an SD card is lower than for a SSD for example). Is the chosen data storage system adequate to the purpose it intends to achieve? Knowing where a storage system is, what it is connected to and who has access to it also gives you keys to better assess risk.

Examples of data transmission systems:

- A hard drive/USB key with a given filesystem (NTFS, exfat, ext4…)
- A SQL database (a software database designed to be accessed using the SQL language)
- A blockchain duplicated across multiple client
- A non-rewritable CD (CDR-R)
- A spreadsheet software such as Microsoft Excel

Potential risks in data storage

Poor permissions management enabling unauthorised access to the data, fallibility of physical hardware storage (e.g. a disk can fail and lose the data it

stored), inadequate data retention capabilities (e.g. blockchain storing data that should be erased), inadequate storage space (e.g. can't store new data because it's full), poor life expectancy (e.g.: choosing a database software management that's not supported by its manufacturer and does or soon will not receive security updates), etc.

iv. Data processing system (software)

Upon capture or after storage, the data can be processed to produce new information. This could be an image analysing software defining what are the objects visible in an image captured, an algorithm giving the solution to a maths problem or a program predicting temperatures based on previously collected data. Data processing systems can either process data on the fly (without storing data in intermediate steps) or use stored data. These systems are usually software developed using a set of programming languages (Java, Python, Go…) and might function in connection with the data storage system. They can run on a variety of devices from a server to a smartphone or a single board microcontroller. Some systems such as neural network-based Artificial Intelligence will perform differently depending on the data they are processing but also on the data they were trained on. In this case it may be worth looking at the training dataset for the AI system as a separate block within the Data collection/capture category. The better you separate the different components the better understanding you'll have of what's at stake.

Why it matters

Data processing systems can produce biased and inaccurate information, both because of the data fed into the system (incomplete, inaccurate, non-representative…) or because of logic flaws (something unaccounted for in the algorithm's logic). Understanding what the processing is designed to do, what data is processed and what type of information it outputs can allow you to spot potential flaws in the code logic, missing variables or to assess how appropriate a system is to make a decision.

Examples of data processing systems:

- A facial recognition software processing photos taken by public cameras
- A boat movement detection software using AI and satellite imagery
- An advertising system that infers your personality traits based on data collected online
- A virtual assistant such as Siri/Google/Alexa

Potential risks in data processing

Flaws in the algorithm logic (something unaccounted for or a human mistake rendering the results false), poor manufacturer support (software/program isn't supported after a certain time making future development and fixes complicated or impossible for the buyer), low transparency/accountability due to licencing (proprietary software make auditing process complicated or impossible), bias due to the dataset it was trained on or data that has been included, security vulnerability (unauthorised access, hack…) etc.

v. A note about prioritising blocks of technology

If you're looking at a specific company or contract, you can use this breakdown and information to focus on the layers where the company is mainly involved. If you are looking at a company specialised in software and data processing (such as Palantir) then you know that this is likely to be the key layer.

That doesn't mean you should neglect the other layers of the technology deployed, on the contrary. These elements, because they are not necessarily part of the company's or public body's expertise might end up being overlooked and poorly managed. For example, the UK stored and ultimately lost covid related data in an Excel file, exposing how little the data storage system had been considered, especially compared to the effort put in collecting this data.

B. ASSESSING NOVELTY/INNOVATIVENESS

Public-private partnerships might very well involve a technology that is well-known and already widely deployed in other contexts, but it might also be a ground for innovation and novelty.

We can identify two main types of innovation:

1. A new technology that isn't widely used or hasn't been deployed in real world context (outside of a lab or a research paper);
2. A new set of features added to an existing technology which greatly expand its performances and capabilities.

Another type of "innovation" may involve deploying existing technologies in new contexts. Assessing these deployments will mostly require identifying governance concerns (Section 4 below).

i. Entirely new technology

In the case of an entirely new technology, the novelty factor is usually obvious as the technology at stake is likely to be little known. New breaking-ground technologies are rare and pose several risks as they haven't necessarily been properly tested or might have unexpected side effects. Approaching an entirely new technology is hard for external actors and it might be difficult to gather relevant information. Nonetheless, there are several common risks that come with innovation and might be worth exploring:

- Disparities between the test environment and the real world impacting the technology efficiency
- Insufficient testing meaning the population it's deployed against is effectively beta testing it
- Overestimation of the technology capabilities and accuracy – the technology doesn't deliver, produces too many errors
- Creation of new problems has been overlooked – this might come from the cost of maintenance, the sustainability of the project in time, the issues

arising from edge cases, or the public body being trapped in a contract that can't be fulfilled by anyone else
- Function creep, the technology can be used for more purposes than it is initially intended for
- Lack of transparency/accountability if the technology is protected by trade secrets and/or under proprietary licencing

ii. New features/capabilities

In the case of an existing technology with new features or capabilities, the innovation might be more difficult to spot but can have an important impact on the use made of the technology. New features and capabilities might come from a technological leap at the hardware or software level. This could be for example with new Computer Processing Units (CPUs) that are much more powerful than the previous generation, or novel technical developments such as quantum computing. For the software side it can be the development of new processing techniques such as the rise of deep learning and equivalent AI solutions.

These innovations can also simply be the addition of an existing technology onto a solution, for example by mounting Radion Frequency sensors to a multitude of small satellites (such as CubeSat), an innovation made possible by the cheap price of these satellites. The risks that arise with the addition of new features or capabilities are more specific and should be easier to identify. Here are some of the risks that arise with such innovations:

- Added capabilities might be unnecessary for the technology to perform its initial function (e.g. equipping body worn cameras with temperature sensors)
- Added capability hasn't been properly tested for the environment it's being deployed in and might yield inappropriate results (e.g. deploying a neural network algorithm for the judiciary system)
- New feature/capability gives the technology a far more intrusive reach (e.g. improving image quality of video surveillance cameras)

- New feature/capability makes the technology much more efficient and enables mass application (e.g. mass interception and processing of internet data)

iii. A note about technical protocols and standards

As mentioned under the *data transmission system* section, protocols and standards might be an interesting thing to look at and understand when trying to take apart a technology. It can give information about whether the technology deployment is taking place in an already developed and standardised environment or trying to define new standards. Here are some useful definitions and standardisation bodies that might be relevant:

Definitions:

- Protocol: a protocol is an agreed language that allows different elements to communicate. One of the most well-known protocol is the internet protocol suite also known as TCP/IP. Protocols are usually standardised and answer to a specific set of rules. They allow any new player in a market to easily develop a product that will be able to use existing infrastructure and communicate with other products. For example, with TCP/IP, anyone can create an internet connected device that will communicate with a server or similar devices around the world.
- Technical Standard: Norm or requirement for a technical task to be operated. Technical standards are more abstract than protocols in that they don't offer hard defined rules for a given programming language or technology. They establish uniform principles, methods and processes that should be followed when developing a technology. The goal is to ensure interoperability between devices and systems (e.g. making sure an external hard drive from a company other than your computer manufacturer will function in any computer). Standards can be developed privately or unilaterally by standardisation organisations. Example: Universal Serial Bus (USB).

Standardisation bodies:

- International Telecommunication Union (ITU): the ITU is a UN organisation in charge of radio communication and standardisation. It works to ensure that countries and private actors agree on standards and protocols to avoid collision and promote development. Standards developed by the ITU are referred to as Recommendations. Some examples of what it does:
    - Manage the radio frequency spectrum (defines which part of the spectrum can be used for what, and by whom, e.g. Wifi and Bluetooth operate between 2400 and 2500MHz);
    - Develop and maintain the Open Document Architecture, an example of a free and open-source standard document file format that any software developer can use for word processing;
    - Publish recommendations regarding armouring of cables to limit interference;
    - Working Groups develop recommendations on topics such as Quantum Information Technologies for Networks and Artificial Intelligence for Assisted and Autonomous Driving.
- Internet Engineering Task Force (IETF): an open standards organization, which develops and promotes voluntary Internet standards, in particular the standards that comprise the Internet protocol suite (TCP/IP).
- International Organization for Standardization (ISO): a standard-setting body composed of representatives from various national standards organizations that publishes worldwide technical, industrial, and commercial standards. Example of standard: ISO 80601 that ensures that thermometers are calibrated the same way in different hospitals.
- W3C: standards organization for the World Wide Web.

Standardisation bodies who have open discussions about standards are interesting (although often hard to penetrate) places to look for lobbying and influence. Private companies or countries might use them as gateways to push a technical solution which might have political consequences. For example, in 2021, the W3C has an "improving web advertising" business group in which Google

suggested a replacement to third party cookies that still enable tracking and targeting.

C. UNDERSTANDING HOW THE TECHNOLOGY AT STAKE FUNCTIONS

Here we identify three main ways of better understanding how a technology works:

i. Added Literature review
ii. Using and testing existing alternatives
iii. Questioning experts

i. Added Literature review

There are several resources available that simplify and popularise complex technologies, starting with Wikipedia. Other resources can be tremendously useful even with little to no technical background, such as semi-specialised press. See for example:

- MIT Technology review (e.g. quantum computing)
- ArsTechnica, (e.g. on NFTS)
- PC Mag (e.g. on 5G Mag)

Academic papers are also an avenue to find information although the language might be less accessible without prior technical knowledge. Nonetheless, it's worth searching on Google Scholar and other resources to find papers on the technology you are looking at, ideally in a similar context to yours or focusing on similar concerns.

Some NGOs with technical resources also publish materials than can guide you in understanding how a particular technology functions and how it can be used in specific contexts, for example:

- Privacy International (tech primer on Bluetooth, GPS)

- EFF (explainer's on Amazon Sidewalk and IMSI catchers)
- Citizen Lab (Analysis of content filtering software on the popular Chinese app YY)

To a certain extent, manufacturers' websites can provide useful insights on the technology you are looking at and how it might function. Technical or promotional documentation for products these companies make can be great tools to understand the specifications of a given technology and provide insights on how it works. You may want to use methods such as Google Dorking to find companies' official brochures and other documents that will help you in your quest.

As with any research, cross referencing what you find, and verifying with more than one source is key to avoid misinformation!

ii. Using and testing alternatives

Trying to find affordable equivalent systems and studying how these work can give you better insight into what goes on within the system you're analysing. If you are looking at facial recognition systems for example, it can be useful to look for open-source projects that you can freely dissect such as this one.

Using these alternatives might require some technical knowledge and not be easily accessible to everyone. Tutorials and guides for beginners can get you a long way to setup and test these systems and should be considered as an easier way to approach this strategy. Similarly, some online course on "how to get started with X" can help you get a clearer understanding of how a technology functions. Introduction chapters of the D2L book on deep learning for example will help you understand the different elements at play in AI technology.

Organisations with technical expertise might also share guides, documentation, and methodologies to use systems they make use of in their work. For example, PI has a Data Interception Environment to analyse traffic from Android apps and has made it available to anyone.

It might be worth looking for other people who have done this sort of testing before, such as experts trying to find flaws or demonstrate bias in a given technology. Joy Buolamwini's work on racist facial recognition systems is a good example of an expert testing a piece of technology to expose its weaknesses.

iii. Questioning experts

After you've done your research there might still be some questions left unanswered, some dots that you are not sure how to connect or simply things you don't have the technical background to understand. Reaching out to experts in academia, specialised press or civil society organisations can be a helpful call in these cases.

When doing so we suggest explaining as clearly as possible what you are trying to do, for what purpose, what you have understood so far and ask questions as precisely as possible. Experts in the field will usually be less interested in giving a lesson about a given technology than helping you understand its application in a specific context. Writing down a list of precise questions you have with details about the context will maximise your chances of getting a response or a call with an expert.

In terms of who you should reach out to, you might want to start by looking at academics that have written papers on the technology you are looking at – in particular, if the focus of their research is one of the key risks you have identified. Alternatively, you can write to professionals working with the given technology as they will usually have a lot of hands-on experience on how it is being used. Looking for people in working groups, exchange groups and knowledge sharing groups is a good first step as it indicates a will to share and learn, increasing your chances of finding someone willing to help you. Asking on specialised online communities such as StackOverflow or Reddit can also get you very relevant information.

Some organisations such as PI also have technologists that you can try reaching out to. They might not have expertise on the technology you are looking at but

could possibly point you in the direction of resources or other people you can talk to.

What our partners say:

Totally understanding the technology you are looking at is hard to achieve. ADC suggests accepting that you can't necessarily know how all the involved blocks work and to try and get your work peer-reviewed to ensure that you are not saying something blatantly wrong. Making sure you have the basics right and that your analysis is based on verified information is more important than trying to understand everything and focusing on details you might have misinterpreted. With that in mind, ADC recommends limiting the scope of your work to a few things and focusing on them.

D. CHECKLIST – UNDERSTANDING THE TECHNOLOGY

This checklist is here to help you ensure you have properly identified the concerns relevant to the technology you are investigating:

- Can you broadly define the technology at stake and what it does?
- What is the role of data in the technology at stake? (data collection system, data transmission system, data storage system, data processing system)
- What are the risks associated with this technology for each particular system?
- How innovative and ground-breaking is the technology?
    - [Optional] What are the risks associated with the innovation factor?
- Can you explain how the technology functions in practice?
    - [Optional] What are the risks associated with the way the technology concretely functions?

4. GOVERNANCE CONCERNS

Through our investigative work and the work of our partners around the world, we have identified a number of persistent governance issues common to public-private partnerships. We have detailed each of our concerns, and relevant corresponding safeguards, here. In this section we provide some high-level guidance on how to identify these types of concerns.

A. UNITED NATIONS GUIDING PRINCIPLES ON BUSINESS AND HUMAN RIGHTS

According to the UN Guiding Principles on Business and Human Rights ('UN Guiding Principles'), companies should respect human rights, meaning they should avoid infringing on the human rights of others, and should address adverse human rights impacts with which they are involved (UN Guiding Principle 11).

The UN Guiding Principles are a set of guidelines for states and companies to prevent, address and remedy human rights abuses committed in business operations. The UN Human Rights Council unanimously endorsed the UN Guiding Principles in its resolution 17/4 of 16 June 2011.

The UN Guiding Principles provide the authoritative global standard for action to safeguard human rights in a business context. As such, in the course of an investigation, they can be used to assess the compliance of a public-private partnership with human rights standards. They can further be used as a resource to advocate for specific actions that companies and governments need to take. In this section, we highlight the key business responsibilities deriving from the UN Guiding Principles and explain how, despite their non-binding character, they have become the norm in assessing human rights responsibilities in business operations.

i. UN Guiding Principles as a standard of conduct for companies

The Guiding Principles contain three chapters, or pillars: protect, respect, and remedy. Each defines concrete, actionable steps for governments and companies to meet their respective duties and responsibilities to prevent human rights abuses in company operations and provide remedies if such abuses take place.

Amongst others, companies are expected to:

- adopt an explicit and public policy commitment to meet their responsibility to respect human rights (human rights policy commitments);
- conduct risk assessments examining the actual and potential human rights impacts, of the proposed tools and services offered (human rights due diligence and impact assessment - HRDD); and
- set up internal accountability mechanisms for the implementation of human rights policies and have process in place to ensure they enable remediation (grievance mechanisms).

The HRDD process includes four core components: identifying and assessing actual or potential adverse human rights impacts that the company may cause, contribute to, or be directly linked to; taking appropriate action and integrating findings from impact assessments across relevant company processes; tracking the effectiveness of measures in order to assess whether they are working; and communicating with stakeholders about how impacts are being addressed and showing stakeholders that there are adequate policies and processes in place.

ii. Technology companies and UN Guiding Principles

The UN Guiding Principles apply to all companies, and therefore apply to the technology sector. However technology companies haven't received the same level of scrutiny as other industries have, notably because of the inherent complexity of their products and services, and because of the novelty of the societal effects they

provoke. The UN B-Tech Project provides authoritative guidance and resources for implementing the United Nations Guiding Principles on Business and Human rights (UNGPs) in the technology space. It was launched in 2019 and is led by the UN Human Rights (Office of the United Nations High Commissioner for Human Rights. See for example "An Introduction to the UN Guiding Principles in the Age of Technology".

In addition, UN Special Procedures and other human rights bodies have been increasingly offering guidance regarding the application of the UN Guiding Principles in the technology sector. See among others the 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, by Dr. Krisztina Huszti-Orbán and Prof. Fionnuala Ní Aoláin, on the "Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?". Also, the 2019 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on "Surveillance and human rights" uses the UN Guiding Principle as a starting point when examining corporate responsibility (A/HRC/41/35).

iii. UN Guiding Principles as the global authoritative standard

The UN Guiding Principles are recognised today as the global authoritative standard on the business responsibility to respect human rights, unanimously endorsed by the UN Human Rights Council in 2011 (Resolution 17/4). While the UN Guiding Principles are not formally legally binding, they are becoming the norm regulating company operations through new national legislation and investor initiatives incorporating them.

1) Basis for national legislation: The UN Guiding Principles have been the basis for the development of new national legislation on corporate responsibility in various countries. In 2017, for instance, the French Parliament adopted a new law imposing a duty of care on multinationals to prevent serious human rights abuses in all their subsidiaries and supply chains (loi de vigilance). Other countries are preparing similar legislative initiatives. Similarly, on 11 June 2021, the German Parliament

passed the "Act on Corporate Due Diligence in Supply Chains" (Supply Chain Due Diligence Act – "Act" or "LkSG"). On 23 February 2022, the European Commission adopted a proposal for a Directive on corporate sustainability due diligence, grounded in part in the UN Guiding Principles.

Other countries and states have implemented due diligence legislation for specific human rights – for example Australia, California, and the UK for modern slavery and the Netherlands for child labour. See an overview of recent developments at the Business and Human Rights Resource Centre.

Also, several countries, including Chile, Colombia, Denmark, Finland, Germany, Netherlands, Norway, Italy, Spain, Switzerland, Tanzania, Thailand, Kenya, Uganda, the UK and the US, have incorporated the UN Guiding Principles in their respective national action plans. A national action plan on business and human rights is a policy strategy to ensure that states adequately protect against negative human rights outcomes for people by business enterprises.

Quite often the application of national legislation extends to business operations beyond the territory of the legislating states. For instance, the EU Directive aims to ensure respect for human rights and the environment throughout the entire supply chain.

2) Responsible investment: The UN Guiding Principles have also been understood as providing guidance for responsible investment. In 2018, a report by the UN Working Group on Business and Human Rights specifically called on investors to implement human rights due diligence as part of their own responsibility under the Guiding Principles, to more systematically require effective human rights due diligence by the companies they invest in, and to coordinate with other organizations and platforms to ensure alignment and meaningful engagement with companies. More and more investors are taking up this responsibility, supported by initiatives like the Investor Alliance for Human Rights and the Principles for Responsible Investment.

B. DATA PROTECTION/PRIVACY CONCERNS

Once you have a good understanding of how a technology works, you may then need to assess its various privacy and data protection implications. To do so, we have outlined here some general aspects of data processing that you can run through to identify any concerns.

There are no universally recognised data protection standards, but regional and international bodies have created internationally-agreed-upon codes, practices, decisions, recommendations, and policy instruments. The most significant instruments are:

- The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981 as amended in 2018;
- The Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980) as amended in 2013;
- The Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72).

Other regional frameworks also exist, including the APEC Privacy Framework – Asia-Pacific Economic Cooperation. And some data protection laws have extra-territorial reach, for example the European Union General Data Protection Regulation (GDPR) applies to controllers and processors who aren't based in the EU, as long as they are processing the data of people who are in the EU, and that processing relates to the offering of goods or services in the EU, or amounts to monitoring their behaviour.

Where a comprehensive data protection law exists, organisations (public or private) that collect and use personal data have the obligation to handle this data according to this law. Please therefore refer to your own jurisdiction's laws, but this section provides an overview of the various things to look out for. However this is not an exhaustive list of all potential data protection concerns - for fuller guidance on data protection, please refer to our full guide.

i. Data sources

The very first step in assessing data processing by a technology is to understand where the data is collected, i.e. where it comes from. You may have identified this at the stage of assessing the technology's data collection/capture system (see tech investigation above), but can supplement this analysis with any documentation about the technology or partnership (e.g. contracts, MoUs, Data Protection Impact Assessments, Data Processing Agreements…), and consider any:

- Datasets/databases that will feed into the technology
- Lists of data subjects or categories of data subjects whose data will be processed (e.g. general members of the public, suspects, victims or witnesses of crime, individuals who live in X area…)
- Sources of data (e.g. will data come from any existing databases, or from particular government departments, authorities?)

Once you understand where the data comes from, you should assess whether the data collection or sharing is lawful (i.e. is it authorised by a lawful basis such as consent of the data subject, or a legal obligation to share this data), and whether this lawful basis is explicitly stated in the documentation. Lawfulness of data collection will depend on the jurisdiction to which the partnership or technology is subject to.

ii. Lawfulness and fairness

Personal data must be processed in a lawful, fair, and transparent manner. This principle is key to addressing practices such as the selling and/or transfer of personal data that is negligently or fraudulently obtained.

Lawfulness means that data must be processed in a way that meets a legal ground for processing. You should assess the lawfulness of processing for each type or category of data that will be processed by the technology, and for each purpose of processing. For example, if data from a database of faces of general

members of the public will be processed to cross-check against a mugshot database, you should assess (1) whether each database was compiled with a lawful ground for processing (note that this requires not only ensuring that the public authority has a lawful ground for collecting the faces in the first place (as addressed by the previous section) and building the database, but also ensuring that if the databases were compiled by a private company, it also had a lawful ground for collecting the data in the first place), and (2) whether the process of cross-checking relies on a lawful ground for processing.

The grounds for processing most commonly found in data protection laws are:

- **Consent** of the data subject
- Necessity of the processing for the performance of a **contract** with the data subject or to take steps to enter into a contract
- Necessity of the processing for compliance with a **legal obligation**
- Necessity of the processing to protect the **vital interests** of a data subject or another person
- Necessity of the processing for the performance of a **task carried out in the public interest** or in the **exercise of official authority** vested in the controller
- Necessity of the processing for the purposes of **legitimate interests** pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject

For further detail on these grounds for processing, please refer to this section of our Data Protection Guide on Grounds for Processing of Personal Data.

Fairness requires that data is not used in ways that data subjects would not reasonably expect, nor in ways that would have 'unjustified adverse effects on them'.

This is a broad principle that should govern all aspects of the processing - the collection of data, the purpose of processing, and the consequences of processing. To assess fairness, you should assess whether the authority controlling the

processing has considered the reasonable expectations of data subjects in light of the context and purpose of processing, the risks to their fundamental rights and freedoms, and the general relationship between the controller and the data subjects (e.g. is there some link or relationships between the two that would make data subjects expect such processing to take place).

iii. Transparency and the right to be informed

Whether processing is fair will also depend in great part on whether sufficient **transparency** about the processing is provided to data subjects. Individuals should be informed when their personal data is being collected, and they must be able to obtain information about its processing. When assessing the deployment of a technology, you should identify whether and through what mechanisms data subjects are informed about the processing of their data.

At the point of data collection, and every time data will be processed for a purpose not envisaged at the time of collection, data subjects should be provided with at least the following **information** (both when they have provided the data directly to the controller, and when the controller has obtained it from another source):

- information as to the identity of the controller (and contact details)
- the purposes of the processing
- the lawful ground(s) for processing
- the categories of personal data that will be processed
- the recipients of the personal data
- whether the controller intends to transfer personal data to a third country and what safeguards are provided for the transfer
- the period for which the personal data will be stored
- the rights of the data subject (such as right of access, right to object, rights to rectify, block and erasure, rights related to profiling and automated decision making, right to data portability)
- the right to lodge a complaint with the supervisory authority

- the existence of profiling, including the legal basis, the significance and the envisaged consequence of such processing for the data subject
- the existence of automated decision-making and at the very least meaningful information about the logic involved, the significance and the envisaged consequence of such processing for the data subject
- the source of the personal data (if not obtained from the data subject)
- whether providing the data is obligatory or voluntary
- the consequences of failing to provide the data
- If individuals are not informed, you should assess whether an exemption to the right to be informed applies. This could be, for example, if denying the right to be informed is necessary and proportionate to prevent or detect crime, for safeguarding national security, or for health, social work, or education purposes. However, any exemption from this right should be provided for in law, and should be justified and supported by a necessity and proportionality assessment. For more details on exemptions please refer to this section of our Data Protection Guide on General Provisions, Definitions and Scope

iv. Data storage and access controls

Once you are satisfied (or not!) that the data will be processed lawfully, fairly, and transparently, you should consider where and for how long the data will be **stored**. The first question to ask is whether the data will be stored on servers held by the public authority, or by the company, or some other third party (e.g. a processor). You might have identified this at the stage of assessing the technology's data storage system (see tech investigation section above). This will affect the distribution of responsibilities for ensuring security of the data and managing access controls.

Personal data, at rest and in transit, as well as the infrastructure relied upon for processing, should be protected by security safeguards against risks such as unlawful or unauthorised access, use and disclosure, as well as loss, destruction, or damage. Please refer to the tech section of this handbook for further details on

what to look out for. Security safeguards should be detailed in the documentation surrounding the partnership, with clear assignment of responsibilities between the public authority, the company, and any third party.

To assess the suitability of access controls, you should consider what kind of access will the company have to data. In particular, if the data is stored on the company's servers, you should check whether the company will have full access to the data, or whether its access will be restricted so that only the public authority has access to it. Although even if the data will be stored on the government's or authority's servers, the company may be granted access, so do check the fine print. Rules about access controls should be provided for in the partnership documentation, with clear and strict exceptions for e.g. emergency access, maintenance access and other.

Contracts sometimes grant companies access to data for things like "improving their services", "performing analytics on their product's performance", etc. You should be wary of these and question exactly what form the company's access will take, and whether it will effectively be benefiting from access to a public authority's database in order to develop its own services, and thereby profit from the partnership beyond the monetary value of the contract.

For more details on exemptions please refer to this section of our Data Protection Guide on Data Protection Principles.

v. International data transfers

You should assess whether the data storage, access or other transfer arrangements will involve data being transferred to another country (e.g. if the contracting company is located in the US). The basic principle is that any transfer of personal data to a third country should not lower the level of protection of individuals' privacy rights. Different jurisdictions have different laws governing how a transfer to a third country can be guaranteed to be "adequate" in terms of rights protections, but you should usually check:

- Has your country/jurisdiction found that the territory where data will be transferred provides "adequate" protection for individuals' rights (i.e. is there what is often called an "adequacy decision" in place)?
- Has the specific transfer been reviewed and authorised by a supervisory authority?
- Is there an agreement in place with standard data protection clauses approved by a supervisory authority?

Exceptions to restrictions on international data transfers may apply. If an exception is purported to apply, it should be provided for in law, and carefully reviewed so that it is not too broadly interpreted or open to abuse, and the transfer remains compliant with human rights standards.

You may consider other issues in relation to international data transfers. For example, if the data that will be transferred is highly sensitive or relating to highly vulnerable populations, even if an adequacy decision or other safeguards are in place, you may want to consider whether the receiving country has laws or practices that allows it to request the data - and therefore whether there is potential harm to individuals if this data ends up in the hands of the receiving country's government.

For more details on exemptions please refer to this section of our Data Protection Guide on The Obligations of Data Controllers and Processors.

C. ACCOUNTABILITY AND OVERSIGHT

Another important aspect of assessing the governance of a public-private partnership requires analysing any accountability and oversight mechanisms in place, including any mechanisms through which the partnership was first established (e.g. public procurement processes).

You should check that certain documents and processes are in place so that the contracting state and company are accountable, that there is proper oversight, and adequate redress mechanisms. Note that you should consider the entire life cycle of the partnership. First at the procurement stage, has the **procurement process** for this contract followed local or international procurement rules? And are those procurement rules adequate? Has there been adequate transparency throughout the procurement process?

Human rights **risk and impact assessments** and/or data protection/privacy impact assessments should normally be performed prior to the award of any contract. They must be performed diligently, following proper templates approved in your jurisdiction or otherwise recognised by global civil society. An example would be The Danish Institute for Human Rights' Human rights impact assessment guidance and toolbox. A proper impact assessment must (in particular, but amongst others) perform a necessity and proportionality assessment that properly considers risks to individuals' rights.

You should then consider whether there is there any independent oversight, which would ensure the partnership remains circumscribed to its stated purpose, to detect abuses or resulting harm, and to require redress. Where and how is this defined and established?

When a public-private partnership is deployed, an **independent oversight body** (e.g. a data protection supervisory authority, an investigatory powers oversight body…) should be designated, to be responsible for (1) reviewing, approving or rejecting new proposals for use of the technology or system deployed as part of the partnership, (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. This independent oversight body should be given appropriate resources (human and financial) to be able to perform its duties.

If these documents and processes have been put in place, they will help you see if the technology deployment is legal, necessary, and whether it's a proportionate response to the issue it's intended to solve. If they haven't, it's important that you try to determine whether the solution is appropriate or if it's overpowered or overreaching – you can, amongst others, write to the relevant public authority to ask that they put these documents or processes in place.

Next you should consider whether the partnership is governed by certain **transparency** standards or legal requirements. If so, are these adequate?

You can then consider how the partners involved will be held accountable with regards to the consequences of the technology deployment. **Accountability** requires that the duties, responsibilities, and standards be defined, appropriate, and assigned amongst parties involved. Are there appropriate mechanisms that enable third parties to scrutinise and challenge the consequences?

Any public-private partnership should be governed by appropriate **policies** governing and documenting the various requirements mentioned above, such as what data will be processed, who has access to data under what conditions, what safeguards must be in place to mitigate risk to individuals, which independent body will be responsible for overseeing the deployment, etc. Such policies should also govern the public authority's use of the technology and define 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. They should also provide **redress mechanisms**, by outlining processes for complaints handling and enforcement of sanctions for violations of the policies, and assigning responsibilities and redress obligations to both the state and the company.

The safeguards we have outlined above are, we believe, a reasonable framework of protections to enforce the responsibilities outlined in the United Nations Guiding Principles on Business and Human Rights, and ensure that public-private surveillance partnerships do not result in human rights abuses.

For further guidance on the various safeguards that should govern public-private surveillance partnerships, please refer to PI's PPP safeguards.

D. CHECKLIST – GOVERNANCE

Data protection and privacy

- Once you've assessed where the data comes from, have you assessed whether the data collection or sharing is lawful?
    - Is this lawful basis explicitly stated in the documentation of the partnership?
- Is the data being collected in ways that people could reasonably expect?
- Have the data controllers considered the risks to the fundamental rights and freedoms of the people whose data will be collected?
- What will the consequences be of people's data being processed in this way?
- Will individuals be informed when their personal data is being collected?
    - through what mechanisms?
    - does an exemption exist in this case? is it justified? is it supported by a necessity and proportionality assessment?
- Are individuals able to obtain information about the data processing?
    - through what mechanisms?
- How long will the data be stored?
- Who will host the data?
- Are there appropriate safeguards protecting data at rest and in transit?
    - Are these detailed in the documentation surrounding the partnership?
    - Is there a clear assignment of responsibilities between the contracting parties?
- What kind of access will the company(ies) involved have to data?
- Will data be transferred across borders?

- If Yes: does the country it is being transferred to have a lower, higher, or same level of protection of individual's rights?
- Has your country/jurisdiction found that the territory where data will be transferred provides "adequate" protection for individuals' rights (i.e. is there what is often called an "adequacy decision" in place)?
- Has the specific transfer been reviewed and authorised by a supervisory authority?
- Is there an agreement in place with standard data protection clauses approved by a supervisory authority?
- If No: is the contract relying on an exemption? Is that exemption provided for in law? Is that transfer compliant with human rights standards?

Accountability and oversight

- Has the procurement process for this contract followed an appropriate procurement framework?
- Is the contract with the company in accordance with national and international standards?
- Is the technology solution necessary and a proportionate response to the issue it's intended to solve?
- Have the company(ies) involved in the contract adopted an explicit and public policy commitment to meet their responsibility to respect human rights?
- Have the parties conducted risk assessments examining the actual and potential human rights impacts of the proposed tools and services offered (human rights due diligence and impact assessments) prior to the award of the contract, and kept these updated during the deployment?
- Does the partnership documentation provide for any independent oversight?
    - Where and how is this defined?
    - Does the oversight body have the appropriate resources to perform its role?

- Are there standards or legal requirements around transparency?
    - Are these standards/requirements adequate?
    - Are these standards/requirements being met?
- Are there any accountability mechanisms for the public body involved in this contract?
- Are there any accountability mechanisms for the private body involved in this contract?
    - Has the private body set up internal accountability mechanisms for the implementation of human rights policies?
    - Does it have processes in place to provide redress?
- Can third parties scrutinise and challenge these accountability mechanisms or their consequences?
- What, if any, are the policies that govern and document any of these requirements?
- Do they include rules regarding the public authority's use of the technology, with clear boundaries for the purpose and use of the technology?
- Are there any redress mechanisms outlined in the contract for violations of these policies? Do they include adequate sanctions and enforcement of those sanctions?

ANNEX: THE HANDBOOK'S CHECKLISTS

This is a collection of each checklist found at the end of each section in the Handbook. You could print these pages only and consult them throughout your research. You can also find just these checklists on PI's website

Uncovering information checklist

- ☐ Have you considered the ethical, legal and security implications of accessing and/or sharing the information you are looking for?
- ☐ Have you considered possible risks and mitigations unique to your context and circumstances?
- ☐ Is the information you are looking for already easily accessible in the public domain?
- ☐ Does the jurisdiction you are interested in have freedom of information or access to documents law that you could use?
- ☐ Are there relevant guides or courses available on how to conduct certain open source research techniques that might help find what you are looking for?
- ☐ Are there any open sources you could access in your country to find the information?
- ☐ Are there any open sources you could access that are located abroad to find the information?
- ☐ Are there any individuals or organisations out there who might be able to help you find the information that you can engage securely?
- ☐ Have your sources given you appropriate and properly informed consent?

- Have you considered how to handle the information you receive from your sources?
    - Where will you save the information?
    - Do you need to anonymise it? Pseudonymise it?
    - Do you need to redact information? How will you do that thoroughly?
    - Are there any contextual details in the information that might point towards your source or anyone else?

Technology under investigation checklist

- Can you broadly define the technology at stake and what it does?
- What is the role of data in the technology at stake? (data collection system, data transmission system, data storage system, data processing system)
- What are the risks associated with this technology for each particular system?
- How innovative and ground-breaking is the technology?
    - [Optional] What are the risks associated with the innovation factor?
- Can you explain how the technology functions in practice?
    - [Optional] What are the risks associated with the way the technology concretely functions?

Data protection and privacy checklist

- Once you've assessed where the data comes from, have you assessed whether the data collection or sharing is lawful?
    - Is this lawful basis explicitly stated in the documentation of the partnership?
- Is the data being collected in ways that people could reasonably expect?
- Have the data controllers considered the risks to the fundamental rights and freedoms of the people whose data will be collected?
- What will the consequences be of people's data being processed in this way?

- Will individuals be informed when their personal data is being collected?
  - through what mechanisms?
  - does an exemption exist in this case? is it justified? is it supported by a necessity and proportionality assessment?
- Are individuals able to obtain information about the data processing?
  - through what mechanisms?
- How long will the data be stored?
- Who will host the data?
- Are there appropriate safeguards protecting data at rest and in transit?
  - Are these detailed in the documentation surrounding the partnership?
  - Is there a clear assignment of responsibilities between the contracting parties?
- What kind of access will the company(ies) involved have to data?
- Will data be transferred across borders?
  - If Yes: does the country it is being transferred to have a lower, higher, or same level of protection of individual's rights?
  - Has your country/jurisdiction found that the territory where data will be transferred provides "adequate" protection for individuals' rights (i.e. is there what is often called an "adequacy decision" in place)?
  - Has the specific transfer been reviewed and authorised by a supervisory authority?
  - Is there an agreement in place with standard data protection clauses approved by a supervisory authority?
  - If No: is the contract relying on an exemption? Is that exemption provided for in law? Is that transfer compliant with human rights standards?

Accountability and oversight checklist

- Has the procurement process for this contract followed an appropriate procurement framework?
- Is the contract with the company in accordance with national and international standards?

- Is the technology solution necessary and a proportionate response to the issue it's intended to solve?
- Have the company(ies) involved in the contract adopted an explicit and public policy commitment to meet their responsibility to respect human rights?
- Have the parties conducted risk assessments examining the actual and potential human rights impacts of the proposed tools and services offered (human rights due diligence and impact assessments) prior to the award of the contract, and kept these updated during the deployment?
- Does the partnership documentation provide for any independent oversight?
    - Where and how is this defined?
    - Does the oversight body have the appropriate resources to perform its role?
- Are there standards or legal requirements around transparency?
    - Are these standards/requirements adequate?
    - Are these standards/requirements being met?
- Are there any accountability mechanisms for the public body involved in this contract?
- Are there any accountability mechanisms for the private body involved in this contract?
    - Has the private body set up internal accountability mechanisms for the implementation of human rights policies?
    - Does it have processes in place to provide redress?
- Can third parties scrutinise and challenge these accountability mechanisms or their consequences?
- What, if any, are the policies that govern and document any of these requirements?
- Do they include rules regarding the public authority's use of the technology, with clear boundaries for the purpose and use of the technology?
- Are there any redress mechanisms outlined in the contract for violations of these policies? Do they include adequate sanctions and enforcement of those sanctions?

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+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).