CANADIAN CIVIL LIBERTIES ASSOCIATION
ASSOCIATION CANADIENNE DES LIBERTES CIVILES

Consultation response: Draft privacy guidance on facial recognition for police agencies

October 21, 2021

Brenda McPhail, Ph.D.
Privacy Director
Canadian Civil Liberties Association
90 Eglinton Ave. E., Suite 900
Toronto, ON M4P 2Y3
Phone: 416-646-1406
www.ccla.org

Lucie Audibert
Legal Officer
Privacy International
62 Britton Street
EC1M 5UY London
United Kingdom
www.privacyinternational.org

Introduction

The Canadian Civil Liberties Association ("CCLA") and Privacy International ("PI") welcome the opportunity to provide this response to the draft privacy guidance on facial recognition for police agencies.

CCLA is an independent, non-governmental, non-partisan, non-profit, national civil liberties organisation. Founded in 1964, CCLA and its membership promote respect for and recognition of fundamental human rights and civil liberties. For fifty years, CCLA has litigated public interest cases before appellate courts, assisted Canadian governments with developing legislation, and published expert commentary on the state of Canadian law. Facial recognition technology engages issues of privacy, surveillance, equality, and potentially other fundamental freedoms, including rights to free expression, assembly and association, which are all core to our mandate.

As a civil society organization, CCLA's perspective on facial recognition technology, or as we often refer to it, facial fingerprinting, is grounded in our mandate to protect the rights and freedoms of individuals. Our experience includes engagement via our international networks in the widespread debates taking place in jurisdictions around the world regarding the risks and benefits that might accrue because of the proliferation of facial recognition applications in law enforcement and national security applications.[1] We are pleased to have the opportunity to collaborate with colleagues from Privacy International in bringing this submission forward for this consultation.

Privacy International ("PI") is a London-based non-profit, non-governmental organization that researches, advocates and litigates globally against government and corporate abuses of data and technology. PI is frequently called upon to give expert evidence to Parliamentary and Governmental committees around the world on privacy issues and has advised and reported to, among others, the UK Parliament, the Council of Europe, the European Parliament, the OECD, and the UN. PI also regularly acts as claimant or intervener in cases involving the right to privacy, having previously acted in the courts of the UK, Colombia, Kenya, France, Germany, United States, as well as in the European Court of Human Rights.

PI regularly engages with authorities in the UK and abroad to warn of the risks of facial recognition technology, and to ensure that any use is lawful and adheres to fundamental rights.[2] Most recently, we filed legal complaints with data protection authorities in five European countries against web scraping and facial recognition company Clearview AI, and against the use of its technology by law enforcement authorities.[3] We welcome the Commissioner's efforts to strengthen the

[1] See, for example, a report published by the International Network of Civil Liberties Organisations, "In Focus: Facial recognition tech stories and rights harms from around the world," Available https://ccla.org/get-informed/inclo-reports/in-focus-facial-recognition-tech-stories-and-rights-harms-from-around-the-world/

[2] See, for example, PI, Submission to the Scottish Parliament's Justice Sub-Committee on Policing's inquiry into facial recognition policing (November 2019), https://privacyinternational.org/sites/default/files/2020-04/19.11.01_JusticeSC_FRT_Evidence_PI_FINAL_2%20%282%29.pdf.

[3] Privacy International (25 May 2021) Privacy International and others file legal complaints across Europe against controversial facial recognition company Clearview AI. Available at https://privacyinternational.org/press-release/4520/privacy-international-and-others-file-legal-complaints-across-europe-against.

framework around police use of facial recognition, and are very grateful to the Commissioner and to the CCLA for this opportunity to contribute our views.

Our responses selectively address questions posed in the notice of consultation.

Framing the Initiative

These guidelines present both opportunity and risk. Canadian law enforcement bodies have been somewhat more cautious in their adoption of facial recognition technology (FRT) than their peers in the United States or the United Kingdom, but as the Clearview AI debacle showed[4], there is significant interest in experimenting with, and integrating this technology into, a range of policing activities in forces across Canada. It is timely for the Office of the Privacy Commissioner of Canada and provincial colleagues to take the opportunity to issue guidance to ensure that the procurement, testing, and use of FRT by police services is compliant with privacy laws, upholds the *Charter of Rights and Freedoms*, and is only undertaken with careful attention to privacy best practice and principles. The risk of issuing such guidelines, however, is that the conversation then shifts to focus on "how" to use the technology in a rights-respecting manner, rather than "if" it is possible to do so. At CCLA and PI, we believe that the question of "if" should still be front and centre in public discussions about this controversial, risky, and often racist technology.[5] This is particularly the case given the Canadian reckoning with systemic racism that followed the murder of George Floyd, which had repercussions in Canada up to and including the revitalization of debates regarding re-tasking and de-funding police.[6]

Consequently, while we respond constructively in this submission to questions regarding the text of the draft guidelines, we wish to state from the outset that we believe there should be a moratorium on FRT for policing purposes in the absence of comprehensive and effective legislation that

- provides a clear legal framework for its use,
- includes rigorous accountability and transparency provisions,
- requires independent oversight, and
- creates effective means of enforcement for failure to comply.

We further take the position that the use of FRT for the purposes of mass surveillance, that is, facial recognition widely deployed in public or publicly accessible spaces to identify individuals,

[4] Joint Investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commisison d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta. PIPEDA Findings #2021-001. Available: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/

[5] The literature in this area is extensive. A seminal piece is Buolamwini, J. & Gebru, T. Proceedings of Machine Learning Research 81, 77-91 (2018); data from the NIST Face Recognition Vendor Test on Demographic Effects is often cited and authoritative, Grother, P., Ngan, M. & Hanaoka, K. *Face Recognition Vendor Test Part 3: Demographic Effects* (NIST, 2019).

[6] A report entitled Rethinking Community Safety – A Step Forward for Toronto, in which CCLA participated with a range of partners under the leadership of the Toronto Neighborhood Centres, examines these issues in depth. Available: https://ccla.org/criminal-justice/ccla-partners-on-report-urging-toronto-to-detask-police/

poses such high potential for abuse, and creates such a serious risk to human rights, that there is no framework, either technical or legal, that could eradicate the threat.[7] We note that the European Parliament, as part of its deliberations around the proposal for an Artificial Intelligence Act[8], has recently voted to support a ban on biometric mass surveillance, and called for a ban on the use of private facial recognition databases.[9]

Responding to the Consultation Questions

Will this guidance have the intended effect of helping to ensure police agencies' use of FR is lawful and appropriately mitigates privacy risks? If you don't believe it will, why?
Can this guidance be practically implemented?

This guidance may help by directing police bodies to consider a series of important factors and core privacy principles across the range of legal authorities relevant to use of FRT. It is rendered necessary yet insufficient by the reality that current Canadian legislation is woefully inadequate to address the potential privacy harms, and harms to rights and freedoms for which privacy serves as a threshold or gateway right, of this technology. And in that statement lies the rub; while the guidance can *help* ensure police agencies' use of FRT is lawful in the current legal landscape, mere legal compliance will be insufficient to fully mitigate the risks to rights, including privacy rights, posed by the full spectrum of potential uses for FR in policing.

This caveat became crystal clear when CCLA had the privilege of participating in a convening hosted by the Information and Privacy Commissioner of Ontario on September 16, 2021, along with representative from police bodies and the Ministries of the Attorney General and Solicitor General. While this blunt summary does something of a disservice to the constructive conversation that occurred, it is not unreasonable to describe a rough split between academic and civil society participants, who wondered if the guidelines went far enough, and those with more direct responsibility for policing who generally expressed concerns that the guidelines went farther in some respects than was warranted by current legislation.

---

[7] In this CCLA and PI are aligned with the 179 signatories to the "open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance." Available: https://www.accessnow.org/ban-biometric-surveillance/

[8] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS (COM/2021/206 final). Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

[9] For the European Parliament's resolution, see European Parliament (6 October 2021) European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)). Available at https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html. For the report adopted by the European Parliament's resolution, see Committee on Civil Liberties, Justice and Home Affairs (13 July 2021) Report on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)). Available at https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.pdf.

This is not a reason for reducing the aspirational aspects of the guidelines or the recommendations based on privacy best practice, including the importance of a necessity and proportionality analysis when considering invasive public surveillance. But it is an indication that practical implementation may be at best, inconsistent. This is particularly the case given that the advice for police bodies to navigate the genuinely complex set of legal authorities including statutory and common law authority for police powers, the relevant federal or provincial privacy laws, and the *Charter of Rights and Freedoms*, is to consult legal counsel. As a pragmatic step, this makes sense. As an effective mitigation strategy to risks to rights, it falls short for two reasons.

First, any such advice will be subject to solicitor-client privilege and as such, will be kept entirely outside the public view. Such advice may be good or great (or neither), it may be effective and strictly adhered to or ignored, it may rely on a rigorous assessment of protections afforded by each legal authority under analysis or come up against the underdeveloped jurisprudence in this area that seems likely to render legal certainty regarding the nuances of FRT use elusive for the foreseeable future. But the public will never know. At best, as with the Cadillac Fairview case, it will require an investigation by the OPC to reveal that there has been a questionable interpretation of privacy law on the part of a private sector actor.[10] At worst, there will be no complaint, no investigation, and no redress for an infringement based on such privileged interpretations. Indeed, the predicted opacity of the legal assessments the guidelines indicate should take place prior to use of FRT would leave the public with no insight into the ways police bodies have given human rights, including privacy rights, due consideration and no means of assessing whether such considerations did or did not carry through into the processes of technology acquisition and use.

Second, in all such cases, there is a genuine question regarding the consistency with which the guidance can be interpreted under such circumstances. In this regard CCLA commends the submission to the current consultation of Professors Lisa Austin and Andrea Slane, who elaborate on the complexity of the legal landscape relevant to FRT use by police.[11] People across Canada deserve equal, consistent, protections for their rights if police forces use FRT. A requirement to "ask your lawyer" in this uncertain legal environment, for this controversial and evolving technology, will not achieve it.

What measures or practices can police agencies implement to help ensure any third parties involved in FR initiatives operate with lawful authority?

[10] While this was a private sector use of facial analytics, not a public sector use of FRT, the principle that permissive or simply incorrect interpretations of law may lead to privacy invasions is relevant in this context. See: Joint Investigation of the Cadillac Fairview Corporation Limited by the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information and Privacy Commissioner for British Columbia. PIPEDA Findings #2020-004, October 28, 2020. Available: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-004/

[11] Lisa Austin and Andrea Slane (October 2021). Submission to consultation on privacy guidance on facial recognition for police agencies.

CCLA believes it is important to stress, firstly, that the guidelines are absolutely correct to place the onus on law enforcement bodies using FRT to ensure the tools they choose are compliant with all relevant Canadian laws. The Royal Canadian Mounted Police's (RCMP) resistance to accepting responsibility for ensuring third party vendors comply with privacy law, documented in the Investigation Findings regarding the RCMP's use of Clearview AI facial recognition technology, clearly highlights the necessity of this provision.[12] It must form a part of every procurement process, carry through to implementation, and continue for the full span of time the tool is in operation. Given the potential for technological changes in third party software, ongoing diligence regarding compliance is of particular importance. Lack of in-house expertise to make such assessments can and should be addressed by independent outside consultation with experts, including a comprehensive range of community stakeholders. In paragraph 69 of the guidance, last bullet point, we would ask that involvement of technical experts and stakeholder groups be considered mandatory instead of a mere option as currently suggested by the wording "may include"; we also suggest that police agencies should be required to demonstrate in their PIA report how they have engaged with such experts and community stakeholders. The guidance should also require that assessment of legal compliance and consultation with external stakeholders must be performed, completed and reported on prior to any trial involving members of the public, and of course prior to any actual contracting and deployment of a technology. The resources to fund such consultation must be considered part of the costs of acquisition and budgeted for accordingly. Bodies responsible for enforcing the law must be demonstrably compliant with the law in all of their dealings if public trust is to be achieved or deserved.

On this topic, PI would like to note that ensuring that third parties involved in facial recognition-related initiatives operate with lawful authority is not the only thing that police agencies should assure themselves of. In its work, PI observes that as authorities around the world seek to expand their surveillance capabilities and harness the power of data to deliver public services, they often have recourse to the services of private technology companies, through public-private partnerships ("PPPs").[13] These partnerships raise serious human rights questions regarding the involvement of private actors in the use of invasive surveillance technologies and the exercise of powers that have been traditionally understood as the state's prerogative.

Through its investigative work and the work of its 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, PI have defined corresponding safeguards that they recommend for implementation by public authorities and companies who intend to enter into such partnerships. Classified between principles of Transparency, Proper Procurement, Legality, Necessity & Proportionality, Accountability, 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. We humbly invite the Commissioner to review these proposed safeguards (and the examples of abuse they seek to remedy) and consider how they

[12] Police use of Facial Recognition Technology in Canada and the way forward: Special report to Parliament on the OPC's investigation into the RCMP's use of Clearview AI and draft joint guidance for law enforcement agencies considering the use of facial recognition technology. June 10, 2021, Office of the Privacy Commissioner of Canada. Available: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/.

[13] PI, Unmasking Policing, Inc., https://privacyinternational.org/campaigns/unmasking-policing-inc.

could be integrated and upheld in this guidance for the use of FRT by police agencies in Canada. The safeguards have not yet been officially launched and we are currently seeking feedback from some of the partners we work with around the world, but please find a near-final draft as **Exhibit 1** to this submission.

Do you foresee any negative consequences arising from the recommendations outlined in this guidance, and if so, what are they?

In our opening comments for this submission, we expressed a reservation that the mere publication of these guidelines, which address "how", more fully than "if", FRT has a role to play in rights-respecting law enforcement, might change the focus of public conversations towards finding the "best" way to enable FRT use by police.

This is particularly important to consider, because while these guidelines are appropriately addressed towards policing bodies, they also have an important role to play in educating members of the public about their rights in relation to FRT. When formally in place, the guidelines will be relied upon by members of the public to develop an understanding of the legal authorities under which police may use FRT, the factors police should be required to assess prior to acquiring FRT, and the safeguards they should put in place to ensure any use of the technology is lawful, ethical and fair.

But there is a serious risk that putting public focus on these "how" questions will forestall or supplant rigorous questioning of the "if" or "when" questions that still have received insufficient attention in Canada. And that matters, a lot, because FRT is genuinely dangerous. Its data source is our faces, the outward signifier of who we are. It can run hidden, behind camera infrastructures that have been in use long enough to be largely invisible by virtue of familiarity, or in conjunction with image databases, such as mugshots, whose collection is governed at least in part under laws that did not contemplate the quantitatively and qualitatively different abilities of FRT in relation to their use.[14] Again, this is particularly relevant in the context of the systemic over-policing of racialized peoples, who are subsequently more likely to be represented in such databases.[15]

FRT is sufficiently powerful that it has the potential to fundamentally change the relationship between residents and the state. It has implications that stretch beyond the confines of public sector privacy law into the social impacts of surveillance, the ethical morass surrounding artificial intelligence, the blurring (or artificially claimed but practically non-existent) boundaries between public and private sector information collection and use, and the interlinked relationships between big data, social sorting and profiling, and discrimination. A strict adherence to a technical, legal definition of privacy grounded in personally identifiable information is profoundly insufficient to address the interlocking risks to those rights which

[14] As, for example, the *Identification of Criminals Act* R.S.C., 1985, c. I-1.

[15] See, for example, Scot Wortley and Maria Jung, "Racial Disparity in Arrests and Charges: An analysis of arrest and charge data from the Toronto Police Service. Submitted to the Ontario Human Rights Commission, July 2020. Available:
http://www.ohrc.on.ca/sites/default/files/Racial%20Disparity%20in%20Arrests%20and%20Charges%20TPS.pdf.

initially rely on an ability to move through the world without routine scrutiny by the state. Yet guidelines that stretch beyond those legal confines will predictably be resisted and will be difficult if not impossible to enforce.

We recognize that there is a rock on one side and a hard place on the other, and these guidelines fit between. The appetite for experimentation with Clearview AI (41 entities in Canada were listed in internal company data as having used the software) speaks to the reality that police forces across the country are interested in moving forward with some form of FRT.[16] In Toronto, the Police Services Board is considering AI policy that encompasses FRT and has used FRT since 2018. Calgary was the first force in Canada to adopt FRT in 2014. Other forces across Canada have allocated funds in their budget, expressed interest in the technology, or have recently finalized contracts with vendors.[17]

The risks of FRT should never be considered by looking only at the technology on its own (as the guidelines do), but always at the context in which it is deployed, and the numerous social goods it threatens. For example, Clearview AI's technology is not a mere searchable face database. It is a dystopian tool that unlocks the ability for anyone to identify anyone both online and in the physical world, and to combine online and physical world information to track, surveil and potentially stalk or harass in much more efficient ways.[18] We of course acknowledge and welcome the Commissioner's finding that RCMP's use of Clearview AI's technology was unlawful, but we worry that a slightly different technology deployed in better adherence to procedural safeguards may check all the boxes in the guidance, while having the same unacceptable effects on fundamental rights.

While careful and comprehensive guidelines, as these are, seem pragmatically better than no guidelines, the risk of their mere existence serving to preclude conversations about whether police should or should not be using FRT at all is real, and troubling. This is particularly the case because conversations in relation to a series of access to information requests submitted by CCLA regarding police use of FRT across the country have indicated that many forces are awaiting the arrival of these guidelines prior to moving forward with acquiring the technology.

---

[16] See Buzzfeed's release of Clearview AI company data, Ryan Mac, Caroline Haskins and Antonio Pequeño, "Police in at least 24 countries have used Clearview AI. Find out which ones here," August 25, 2021, available: https://www.buzzfeednews.com/article/ryanmac/clearview-ai-international-search-table.

[17] York Regional Police allocated 1.68 Million dollars for a "Facial Recognition and Automated Palm and Fingerprint Identification System", Regional Municipality of York Police Services Board, Revised Agenda Public Session, November 7, 2018, http://www.yrpsb.ca/usercontent/meetings/2018/nov/Merged_Agenda_Package_-_Public_Board_Meeting_Nov07_2018.pdf.; Alberta's IPC is on record encouraging Edmonton Police to seek a privacy review for their intended FRT program, see Jordan Omstead, "Caution urged as Edmonton police explore facial recognition technology," CBC News , February 5, 2020, https://www.cbc.ca/news/canada/edmonton/caution-urged-as-edmonton-police-explore-facial-recognition-technology-1.5451823; and the Sûrete du Québec finalized a contract with IDEMIA Identify and Security Canada for $4.4 million in August 2020, see Kevin Dougherty, "Quebec lawmakers raise the alarm over police use of facial recognition," iPolitics, September 22, 2020, https://ipolitics.ca/2020/09/22/quebec-lawmakers-raise-the-alarm-over-police-use-of-facial-recognition/

[18] Privacy International, Get out of our face, Clearview!, https://privacyinternational.org/campaigns/get-out-our-face-clearview.

There is the related risk that the guidelines, once implemented, will also serve to lessen the urgency for a badly needed new legal regime to govern the collection and use of biometric identifiers in Canada.

In this context, PI would like to draw the Commissioner's attention to the repercussions of a judgment from the Court of Appeal of England & Wales in the case of *Bridges v South Wales Police*.[19] The Court found in this case that the deployment of Automated Facial Recognition technology by the South Wales Police breached a number of data protection laws and equality laws, and that there were "fundamental deficiencies" [20] in the legal framework surrounding the use of the technology. While we welcomed this judgment, we have observed various police forces later rely on it as providing that their use of facial recognition technology can be lawful if they develop better policies, such as to "who" can be placed on a watchlist and "where" the technology can be deployed. Police forces in the UK have thereby not been deterred from using the technology and some are currently deploying live facial recognition technology.[21] We therefore worry that despite numerous strong statements about the dangers of FRT and need for necessity and proportionality in its use, "easy-to-fix" concerns and guidance on how to fix them actually detract from engaging in the more serious and fundamental questions about the place of such a technology in democratic societies.

Is police use of FR appropriately regulated in Canada under existing law? If not, what are your concerns about the way police use of FR is currently regulated, and what changes should be made to the current legal framework?

The CCLA submits that police use of FRT is not appropriately regulated in Canada under existing law. The patchwork of legal instruments deemed relevant in the guidelines is insufficient in oversight provisions, insufficient in enforcement options, and insufficient to protect the fundamental rights threatened by biometric surveillance, including privacy, freedom of expression, freedom of association, and equality.

A cross-sector data protection law grounded broadly in a human rights framework would come closer to the mark, particularly in an environment where the private and public sector are using the same technologies (albeit often to different ends) but are now subject to different legal requirements. Targeted laws governing biometrics or more broadly, data-intensive algorithmically enabled or driven technologies could be even better fit for purpose, and there are a number of examples globally where such legislation has recently been enacted or is under consideration.[22] In Canada, we already have a specific statute governing police use of DNA, so

[19] *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058. Available at https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment-1.pdf.
[20] Ibid, para 91.
[21] See Metropolitan Police, Live Facial Recognition. Available at https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition/.
[22] See for example the Illinois Biometric Privacy Act, 740 ILCS 14; New York Senate Bill S79; and Vermont S.124 (Act 166) An act relating to governmental structures protecting the public health, safety and welfare.

the precedent has been established with regards to a data of a highly sensitive and personal nature.[23]

Oversight

Accountable surveillance, a term used in a recent article by the UK Surveillance Camera Commissioner's Office (itself an example of a possible model), is increasingly necessary to enforce in a world where new options for tracking, monitoring, and identification proliferate.[24] There is a dearth of effective, independent oversight (not just review) and public transparency requirements in the current legal framework that leaves significant accountability gaps.

A key factor is a comprehensive oversight mechanism for police use of surveillance technologies that brings a range of perspectives, including from law enforcement and civilian stakeholders, to bear on the full suite of questions relevant to considering potential use of FRT and other invasive, data-driven surveillance technologies. In this regard the CCLA adopts the suggestions regarding "Crafting an Oversight Framework that would be Adequate" contained in the submission to this consultation by Professors Austin and Slane for the creation of an independent, external oversight body and correlated processes.[25]

Enforcement

Enforcement is an area amenable to improvement within current privacy laws. While policing is a provincial responsibility and most police forces are governed by provincial or municipal privacy laws, federal laws govern the RCMP. Here we address only required improvements to the relevant federal privacy legislation.

The Office of the Privacy Commissioner of Canada, alone and together with the provincial Commissioners, has recently engaged in three investigations regarding facial analytic and facial recognition technology, and made detailed findings. In each of these cases, there were provisions in our current federal public and private sector laws that applied and allowed for pointed findings, but no consequences beyond naming and shaming. In each case, those under investigation pushed back or disputed recommendations, and the lack of enforcement powers, including a lack of binding order-making powers, for the federal Commissioner meant no administrative penalties could be applied. Bill C-11 would not have solved this problem and it remains to be seen whether the next private sector privacy law proposed will be fit for this purpose.

The recent consultation regarding modernizing Canada's Privacy Act posed questions regarding the need to provide the Privacy Commissioner with the power to issue orders, expand the Federal Court's review jurisdiction to encompass matters relating to the collection, use, disclosure, retention and safeguarding of personal information, and adding new offences for serious

[23] DNA Identification Act (SC 1998, c. 37).
[24] Surveillance Camera Commissioner's Office, "What we talk about when we talk about biometrics…*", 12 October 2021. Available: https://videosurveillance.blog.gov.uk/2021/10/12/what-we-talk-about-when-we-talk-about-biometrics/.
[25] Austin and Slane (October 2021). P. 4

violations of the Act.[26] These measures are necessary for the OPC's review function of Canada's national police force, the RCMP, to gain in effectiveness.

Fundamental Rights Protections

There are risks to rights inherent in FRT, and more broadly speaking, algorithm-driven decision making, inferential algorithms, and a range of other potential biometric technologies that may be used to facilitate remote surveillance, and whose impacts go beyond privacy to potentially infringe a wide range of *Charter*-protected rights. A focus on regulating the use of individual, personally identifiable information cannot fully mitigate these risks, which may also adhere to groups who are socially sorted using a range of personal and inferred data, and subject to differential treatment as a result in ways that may be subtle and cumulative rather than direct and focused. The recommended range of perspectives necessary to consider when determining how to regulate the diffuse and socially corrosive impacts of unrestrained surveillance is well expressed by the current Surveillance Camera Commissioner in the UK:

1. The technologically possible (what can be done)
2. The legally permissible (what must/must not be done) and
3. The societally acceptable (what communities will tolerate and support).[27]

The need for a framework to support fundamental rights protections beyond the scope of privacy rights alone supports the call for an independent, external, multidisciplinary oversight body for police use of data-driven surveillance technologies including FRT, as per the recommendation above.

Should police use of FR, including the collection of faceprints, be limited to a defined set of purposes (such as serious crimes or humanitarian reasons, e.g. missing persons)? Should they be able to use or retain faceprints beyond those of individuals who have been arrested or convicted?

FRT should be unlawful if deployed in bulk/indiscriminately (i.e. taking a mass surveillance approach).

Are there circumstances in which police should never be allowed to use FR, or specific applications of FR that should not be permitted (i.e. 'no-go zones' such as the indiscriminate scraping of images from the Internet)? Should there be special rules for (or a prohibition against) the application of FR to youth?

[26] Government of Canada. "Respect, Accountability, Adaptability: A discussion paper on the modernization of the *Privacy Act*. Available: https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/raa-rar.html#s1

[27] Fraser Sampson. *Response to the Government's Statutory Consultation on the Surveillance Camera Code under s. 29(5)(e)*. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1017674/Fraser_Sampson_s_response_to_SC_Code_Revision_FINAL_08.09.2021.pdf

One 'no-go-zone' would also be the use by police agencies of privately deployed FRT systems and watchlists. For example, PI last year denounced the partnerships between police forces in the UK and the company Facewatch, which sells FRT software to retail stores and other businesses and allows them to upload pictures of "subjects of interest" ("SOIs") so they are alerted when these enter their premises.[28] Facewatch even centralizes the lists of SOIs that their subscribers upload and may share them with surrounding subscribing businesses. The issue with such a partnership is two-fold: (1) it puts policing powers in the hands of private actors, allowing them to decide who is a suspect or potential criminal; and (2) it expands the realms of surveillance in allowing the police to extend the reach of its surveillance to private spaces. We invite the Commissioner to warn about the use of such public-private partnerships which tend to skirt established procurement procedures and to operate outside the legal framework governing policing powers and refer in this regard to the proposed safeguards in **Exhibit 1** (as introduced above).

CCLA notes that this question, and the others which address specific permissions and protections for FRT uses (i.e. What protections should be granted to individuals whose biometric information is included in a faceprint database? Should police use of FR, including the collection of faceprints, be limited to a defined set of purposes (such as serious crimes or humanitarian reasons, e.g. missing persons)? Should they be able to use or retain faceprints beyond those of individuals who have been arrested or convicted?) are precisely the kinds of questions that Canada needs a multistakeholder, statutorily created, independent oversight authority to consider, as per our recommendations and those of Austin and Slane in the "oversight" section above. Drawing on inspiration from the recently legislatively created Vermont Criminal Justice Council with regards to FRT policy,[29] such questions require careful consideration by a multidisciplinary group with the dedicated time, resources, and specific mandate to engage with the full range of stakeholders to determine the correct answers, for people in Canada, now and for the future.

CCLA further recommends, as is the case in Vermont, a moratorium on facial recognition technology by law enforcement officers until such time as the suggested oversight body has had the chance to consider and answer these and other questions, and made its recommendations for a federal/provincial/territorial policy on law enforcement acquisition and use of FRT.

Are there any other important policy issues that should be addressed in relation to police use of FR?

This includes, for example, emerging legal, ethical, or social issues in relation to

[28] Privacy International (15 October 2020) Facewatch: the Reality Behind the Marketing Discourse. Available at: https://privacyinternational.org/long-read/4216/facewatch-reality-behind-marketing-discourse.

[29] See Vermont S.124 (Act 166) An act relating to governmental structure protecting the public health, safety and welfare, s. . October 7, 2020. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1017674/Fraser_Sampson_s_response_to_SC_Code_Revision_FINAL_08.09.2021.pdf

the development and implementation of faceprint databases by the police. If so, what are these issues, and how do you recommend they should be addressed?

Felix Stalder, in an opinion piece aptly entitled "Privacy is not the antidote to surveillance" notes that surveillance is "a structural problem of political power."[30] We give our law enforcement agencies extraordinary powers, of investigation, arrest, and detention to enforce the rule of law. In turn, effective accountability and transparency must form a key part of the structure that upholds police in their powers. FRT and other data-intensive surveillance technologies have the potential to obliterate privacy, to render it impossible to move through public space unwatched, uncategorized, unidentified.

It is reasonable to note here, in a closing section on emerging issues in relation to the development of faceprint databases by police, Woodrow Hartzog and Evan Selinger's five distinguishing features of FRT that differentiate it from other biometrics, and other data-driven surveillance technologies. First, they note, faces are hard to hide, hard to change, cannot be encrypted and are remotely capturable covertly and from a distance. Second, there is an existing set of legacy databases containing images, including driver's licenses, passports, mugshots, social media profiles, all created for other purposes, legally authorized or consensual, all potentially able to be leveraged. Third, data inputs are images that are easily collected by current technology—CCTV cameras, body cams, dash cams—tools in the field right now. This can happen behind the camera technology the public sees and knows about, invisibly. Fourth, he identifies the risk of "tipping point creep" as a shift from static, after the fact analysis to live, precautionary analysis is technologically relatively simple and likely as social acculturation to the technology occurs. Finally, faces are part of our core identity, online and off, connecting what Hartzog and Selinger call our "real-name, anonymous, and pseudonymous activities."[31]

These five features put the potential structural power of FR technology, wielded by law enforcement, into stark relief. FRT uses our face against us in policing contexts. It can, and generally will, happen covertly. It builds on a range of legacy databases; mugshot databases in particular carry their own legacy due to the well-documented disproportionate arrest and charging of those who are Black and Indigenous.[32] It can be live or retroactive; if the latter, any image taken at any time in any circumstance could be used as a comparator in contexts where even if the acquisition was "lawful" at the time and in the circumstances, might have occurred without any public understanding or anticipation of such a use.

There is a disturbing trend in conversations regarding law enforcement use of FRT to talk about "uncontroversial" or even "common" uses such as comparisons of captured images with a mugshot database, as opposed to "controversial" uses such as using FRT live in public spaces. But current uses are not "uncontroversial," law enforcement bodies have simply gotten away with thus far. For example, in Toronto it began with a secretive pilot project that went public when a journalist noticed a report in a set of technically public, but practically obscure, Police

[30] Felix Stalder, (2002). "Opinion. Privacy is not the antidote to surveillance." Surveillance & Society. Available: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3397/3360

[31] Woodrow Hartzog (August 2, 2018). "Facial Recognition is the Perfect Tool for Oppression." Medium. Available: https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66

[32] Supra, note 7.

Board Minutes. By the time it came to light, The Toronto Police Service had already decided to proceed with a full implementation of the technology.[33] There may be a spectrum of uses, a concept that emerged at the previously mentioned Ontario IPC roundtable, but there is no part of that spectrum that is free of privacy risks or pressing social questions about discriminatory impacts.

Canada needs a public debate about FRT. The conversations around the guidelines that are the subject of this consultation have begun that process, but only among a small group of law enforcement groups, civil society actors, academics and privacy regulators, not our democratically elected representatives, and not the broader public. More is needed. As a next step to this consultation, CCLA believes the OPC is well positioned to initiate and lead some of those necessary public consultations, which must include a component of public education.

Both the CCLA and PI are grateful for the opportunity to make this submission and look forward to ongoing conversations on facial recognition technology and its appropriate constraint and regulation.

[33] See Kate Allen and Wendy Gillis, (May 28, 2019) Toronto police have been using facial recognition technology for more than a year. Available: https://www.thestar.com/news/gta/2019/05/28/toronto-police-chief-releases-report-on-use-of-facial-recognition-technology.html

Exhibit 1

SAFEGUARDS FOR PUBLIC-PRIVATE PARTNERSHIPS

October 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, Procurement Procedures,

Legality, Necessity & Proportionality, Accountability, 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 from across the world of abuse and of successful advocacy against surveillance partnerships.

The United Nations ('UN') Guiding Principles on Business and Human rights (the '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, ("UN Guiding Principles" or "UNGP"). 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.

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 required to obtain limited and restricted	Palantir and the UK government: information about Palantir's collaboration with UK government departments has	**All PPP documentation should be made publicly available** – and where legitimate concerns around disclosure of sensitive information arise (such as state secrets or national security information), it should be made available on a confidential basis

[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; 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)
	responses to requests for information	been very limited. PI and other CSOs have repeatedly attempted to obtain further information but were given little additional and sometimes contradictory information.[5]	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 provided, some assessments may or may not be required): • Contracts, procurement information, Memorandums of

[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)
			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" prevent disclosure of details of a technology or system	Amazon and the NHS: the contract obtained was largely redacted for reasons of Amazon's commercial	Companies involved in PPPs should waive commercial confidentiality and make their technologies to **fully auditable**, for third parties to be able to understand (1) what data the company and its technology have access to, (2) how the technology analyses the data and draws conclusions, and (3)

	Issue	Example(s)	Safeguard(s)
		interest.[8] After PI's challenge, the UK's Information Commissioner's Office (ICO) ordered partial disclosure.[9]	what role the technology performs in the public authority's decision-making process. Such information should be available for 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 be processing – the public contract only mentioned processing of data on	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 that authorities have not properly reflected on the impact of the processing) • Types of personal data, with purposes of processing for each

[8] Privacy International, Alexa, what is hidden behind your contract with the NHS?, 6 December 2019, available at https://privacyinternational.org/node/3298.
[9] See 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.

	Issue	Example(s)	Safeguard(s)
		"members of the public".[10]	• Sources of personal data (where the data will be obtained) and legal basis for obtaining from each of those sources
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.[11]	**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.
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	**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

[10] 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.
[11] See PI, 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)
		defined entity was designated as responsible to respond to our requests.	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.

II. PROPER 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 against 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 process; and/or exceptions from	Peru En Tus Manos: in Peru, a Covid-19 tracking app, was encouraged for	When awarding a contract to a company, public authorities must demonstrate adherence to **formal public procurement processes**, and must put in place **formal**

	Issue	Example(s)	Safeguard(s)
	such formal processes for national security issues	use by the Peruvian government despite no formal approval process having been gone through.[12] Palantir's original £1 contract with the NHS for the Covid datastore was struck without proper scrutiny and adherence to procurement processes.[13]	**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 DPIAs or PIAs and HRIAs, or those assessments not being conducted diligently	Facial recognition in Argentina: the UN SR on Privacy expressed concerns that two cities deployed facial recognition	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.[16] [17]

[12] See 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.

[13] The Bureau of Investigative Journalism, Revealed: Data giant given 'emergency' Covid contract had been wooing NHS for months, 24 February 2021, https://www.thebureauinvestigates.com/stories/2021-02-24/revealed-data-giant-given-emergency-covid-contract-had-been-wooing-nhs-for-months.

[16] 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.

[17] 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 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.

	Issue	Example(s)	Safeguard(s)
		and other surveillance software without carrying out any PIAs, and no one was able to explain their necessity proportionality.[14] 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.[15]	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.[18] 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.[19] Where algorithms will be used to make automated decisions, AIAs ought to be performed as well.[20]
8	DPIAs conducted as post-award compliance checkbox rather than pre-award decision tools	Huawei in Como: DPIA conducted only after tender awarded to A2A Smart City.[21]	Individual DPIAs should be conducted during the procurement process when evaluating different technologies and companies' ongoing services, and the results from those DPIAs should be taken

[14] 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).
[15] 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.
[18] 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.
[19] 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/.
[20] 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.
[21] See n 15.

	Issue	Example(s)	Safeguard(s)
			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.[22] Gamma International found by the UK NCP to have insufficient CSR policies and human rights due diligence practices.[23]	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.
10	Technologies deployed for private purposes	Amazon Ring has agreements with law enforcement	As a principle, **public authorities should not systematically use surveillance and mass data**

[22] See 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.
[23] 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)
	are sometimes co-opted by public authorities for policing purposes, without required public procurement processes and safeguards	agencies around the world granting them access to private surveillance networks.[24] Facewatch systems deployed for retail surveillance offered for use by police forces.[25] Facial recognition in London King's Cross station – FRT installed for private security purposes, later used for policing.[26]	**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.

[24] See PI, One Ring to watch them all, 25 June 2020, available at https://privacyinternational.org/long-read/3971/one-ring-watch-them-all.
[25] 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.
[26] See PI, 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."[27] 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.[28]

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 human rights obligations,	Thomson Reuters data sold to Immigration and Customs Enforcement (ICE), a US agency reported to have separated children from their parents and detained them in horrifying conditions.	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 accountable for any

[27] Office of the UN High Commissioner for Human Rights, Who Will Be Accountable? Human Rights and the post-2015 Development Agenda, Summary, 2015.
[28] 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)
	while private companies may not always be bound by these same laws	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.[29]	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.**[30] This should be explicitly provided for in the documentation governing the partnership.[31]
12	Technologies developed in one country supplied to another country with differing human rights standards	Chinese government working with Chinese surveillance firms to develop facial recognition technology standards considered repressive (e.g. incorporating ethnic tracking) – those same technologies are then exported.[32]	PPP documentation should append (an) **agreed-upon human rights framework(s)** which shall govern the partnership and be used throughout 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.

[29] 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/.
[30] 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."
[31] The UN Guiding Principles on Business and Human Rights provide 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." (UN Guiding Principle 5).
[32] 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.

	Issue	Example(s)	Safeguard(s)
		Telecoms companies providing Lawful Intercept telecommunications infrastructure developed for EU standards to regimes with differing or no human rights standards.[33]	Companies should refuse to provide their products or services to a state they are aware does not respect international human rights standards.[34]
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.[35]	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.[36] Any use of the technology that does not comply with this policy should undergo a new approval process determining whether the new use can adhere to the technology use policy, and if not, a separate use policy should be developed for that new use.

[33] 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.
[34] The UN Guiding Principles require companies to consider the potential use of their products as part of their human rights due diligence.
[35] 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.
[36] 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)
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".[37] The PCAP is advisory only, members are compensated for their time, and its discussions are confidential.[38] NSO previously pledged to engage in consultations with human rights experts on its practices, but the identity of experts and content of advice received was never made public.[39]	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.
15	Reliance on data-driven technologies has been shown to entrench inequalities, inaccuracies and injustice, without	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.[40]	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

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

	Issue	Example(s)	Safeguard(s)
	providing ability to question the decisions they make or lead their users to make		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.

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".[41] In addition, international human rights law requires that any interference with the right to privacy must be necessary and proportionate.[42] 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.[43] 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."[44]

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 appropriate legal framework	Mobile Phone Extraction (MPE) technology has been deployed by police forces in	When considering the need for, and the deployment of a technology to address a public need or fulfil a public function, the state must consider whether **an appropriate**

[41] 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.
[42] 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 […]").
[43] UN Human Rights Committee, General Comment No. 34 (Article 19 ICCPR), 12 September 2011, para 35.
[44] OHCR Report on the Right to Privacy in the Digital Age (n 42), para 23.

	Issue	Example(s)	Safeguard(s)
	authorising and governing their use	the UK for years without a proper legal framework.[45]	**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.[46]	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 independent evidence sources and comparative practices.

[45] See 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.
[46] 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)
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.[47]	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.

[47] See Wired and Privacy International (n 15).

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."[48]

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."[49] 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	The use of mobile phone extraction technology by police forces in the UK went on for years in ways the ICO later found	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 investigatory powers) responsible for (1) reviewing, approving or rejecting

[48] UN Guiding Principle 5.
[49] 2009 Report of the UN Special Rapporteur on Counter Terrorism (n **Error! Bookmark not defined.**), para 62.

	Issue	Example(s)	Safeguard(s)
		inappropriate and unlawful.[50]	new proposals for use of the technology or system deployed as part of the PPP, (2) undertaking regular 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.[51] 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 for law enforcement.[52]	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' rights throughout the deployment's lifecycle.

[50] 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.
[51] 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." (para 2.26).
[52] See Privacy International (n 24).

	Issue	Example(s)	Safeguard(s)
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 solely positive view of FRT.[53]	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.[54] 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.

[53] 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.
[54] 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 (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.[55] 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".[56]

In the context of surveillance or processing of personal data, the secrecy around technologies used render 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".[57]

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

[55] 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.

[56] 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.

[57] 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.

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 not cooperating with efforts to obtain accountability and redress.[58]	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 company involved, and ought to adhere to the eight "effectiveness

[58] 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)
			criteria" set out in UN Guiding Principle 31. The state should also ensure that the company they contract with has a grievance mechanism in place,[59] 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.[60] Palantir and the NYPD: at the end of the contract, Palantir refused to produce the analysis generated by Palantir's software for it to be transferred to a new non-Palantir system.[61]	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 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

[59] This is required by UN Guiding Principle 29.

[60] 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.

61 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.

	Issue	Example(s)	Safeguard(s)
			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.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org