Privacy International's response to the call for input for the Report of the High Commissioner for Human Rights on "The impact of arms transfers on human rights"

January 2024

Introduction

Privacy International (PI)[1] welcomes the opportunity to provide input to the report by the UN High Commissioner for Human Rights on the impact of arms transfers on human rights (the Report). We note that the Report will cover all aspects of the Human Rights Council resolution 53/15 adopted on 13 July 2023 (the Resolution), with a focus on the role of access to information in preventing, mitigating and responding to the negative human rights impact of arms transfers.

PI has extensive experience of access to information procedures in various countries. Most freedom of information (FOI) laws contain a presumption in favour of disclosure, with exemptions applied as restrictively as possible. But we submit that in our experience exemptions to FOI laws are widely used by public authorities to prevent disclosure of information and documentation concerning details of procurement, deployment, use and evaluation of arms transfers and other transfers of equipment and capabilities to other countries. They are difficult and onerous to challenge. Civil society organisations and individuals seeking release of information are in an inherent position of power and information imbalance.

In the following pages, our submissions highlight common threads identified throughout our and others' experiences of navigating access to information regimes, including: (1) severe, systematic and unlawful delays in the provision of information; (2) unsubstantiated, blanket application of exemptions; (3) blanket application of exemptions to entire documents rather than granular application of redactions; (4) costly and time-consuming

[1] Privacy International (PI) is a London-based non-profit, non-governmental organization (Charity Number: 1147471) that researches and advocates globally against government and corporate abuses of data and technology. It exposes harm and abuses, mobilises allies globally, campaigns with the public for solutions, and pressures companies and governments to change.[1] PI challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy. Within its range of activities, PI investigates how peoples' personal data is generated and exploited, and how it can be protected through legal and technological frameworks. It has advised and reported to international organisations like the Council of Europe, the European Parliament, the Organisation for Economic Cooperation and Development and the UN Refugee Agency.

processes of appeal to supervisory authorities; and (5) over-application of commercial interests and intellectual property exemptions governed by contractual provisions with commercial partners rather than in accordance with the law.

The role of access to information in preventing, mitigating and responding to the negative human rights impact of arms transfers

PI regularly uses FOI laws to obtain documents and information for its research purposes. It has proved an essential tool to better understand authorities' procurement processes, decision-making processes, policies, risk assessments, commercial relationships, etc. Disclosures of human rights impact assessments (HRIA) or data protection impact assessments (DPIA) in particular are key to obtaining useful details of deployments of new technologies, equipment, etc, and understanding their impact on fundamental rights.

Successful efforts by PI to access public information have led to identification of the human rights impact of surveillance technology deployments, determination of abuses, as well as it enabled transparency, accountability and redress.

In 2020 for example, PI obtained disclosures from European Union (EU) bodies such as the European Commission, EU Agency for Law Enforcement Training (CEPOL), Frontex and the European External Action Service (EEAS),[2] revealing amongst others:

- Training delivered to police and security agencies in the Balkans, Middle East and Norther Africa on controversial phone and internet surveillance techniques;[3]

- Training and equipping of border and migration authorities in non-member countries with surveillance tools, including wiretapping systems;[4] or

- The involvement of security companies in technology deployments in third countries, such as the deployment by Civipol (a French security company) of mass biometric systems in Western Africa used to stop migration and facilitate deportations, without adequate risk assessments.[5]

These disclosures provided a strong body of evidence that enabled the filing of a joint complaint by PI and 5 other human rights organisations to the European Ombudsman, calling for an investigation into EU surveillance aid to non-EU countries. The Ombudsman's

[2] PI, Surveillance Disclosures Show Urgent Need for Reforms to EU Aid Programmes (10 November 2020), https://privacyinternational.org/long-read/4291/surveillance-disclosures-show-urgent-need-reforms-eu-aid-programmes.
[3] PI, Revealed: The EU Training Regime Teaching Neighbours How to Spy (10 November 2020), https://privacyinternational.org/long-read/4289/revealed-eu-training-regime-teaching-neighbours-how-spy.
[4] PI, Borders Without Borders: How the EU is Exporting Surveillance in Bid to Outsource its Border Controls (10 November 2020), https://privacyinternational.org/long-read/4288/borders-without-borders-how-eu-exporting-surveillance-bid-outsource-its-border.
[5] PI, Here's how a well-connected security company is quietly building mass biometric databases in West Africa with EU aid funds, https://privacyinternational.org/news-analysis/4290/heres-how-well-connected-security-company-quietly-building-mass-biometric.

investigations into the EU Emergency Trust Fund for stability and addressing root causes of irregular migration and displaced persons in Africa (EUTFA) concluded that the European Commission had not, but should have, conducted human rights impact assessments prior to transfers of surveillance capabilities.[6] The "major governance issues" and "poor human rights records" of many of the countries in which the EUTFA projects were implemented increased the risk of human rights violations and would have warranted such assessments. The European Ombudsman therefore suggested that the Commission's guidelines concerning the evaluation of aid projects, both in Africa and elsewhere, "should require that an assessment of the potential human rights impact of projects be presented together with corresponding mitigation measures".

FOI disclosures are therefore crucial in revealing details of states' equipment and capability transfers. They enable scrutiny by experts, civil society, oversight bodies and the wider public, sometimes leading to (as in this case) recommendations for improvement of assessment and mitigation of human rights impacts.

Exemptions to access to information laws

Access to information and documents laws and policies all contain exemptions to the duty to provide access to information, in order to preserve various interests. UK law for example, under the Freedom of Information Act (FOIA) 2000, allows refusal of access to a document for the following reasons (amongst others):

- Information supplied by, or relating to, bodies dealing with security matters (s.23)
- National security (s.24)
- Defence (s.26)
- International relations (s.27)
- The economy (s.29)
- Law enforcement (s.31)
- Formulation of government policy (s.35)
- Prejudice to effective conduct of public affairs (s.36)
- Commercial interests (s.43)

Similar exemptions apply for access to documents held by EU institutions, under Article 4 of Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

While the presumption is in favour of disclosure, PI's experience across countries has been of an over-application of exemptions when disclosure is inconvenient or uncomfortable for the disclosing authority, or when a commercial party is involved. Here we provide a few examples of the exemptions most commonly invoked in response to our FOI requests.

[6] Emily O'Reilly, European Ombudsman,

Blanket national security exemptions

National security exemptions are the ones applied with least substantiation, often constituting "absolute exemptions" that aren't subject to any public interest test. PI has never managed to obtain disclosure of national security-related information, even after requests for reviews and appeals of exemptions.

In the UK, for example, section 23 of the FOIA 2000 disapplies the disclosure duty on all "bodies dealing with security matters", and section 24(2) disapplies the duty if an exemption is "required for the purpose of safeguarding national security". This is in contrast with most other exemptions, which require the authority to weigh the public interest in maintaining the exemption against the public interest in disclosure – the "public interest test", or "PIT". In essence, all state bodies dealing with security matters are exempt from access to information obligations, making scrutiny over transfers of arms or other security equipment particularly difficult if not impossible.

In 2013, PI made a FOI request to the UK's Foreign & Commonwealth Office (FCO) and Government Communications Headquarters (GCHQ), the signals intelligence agency. We sought disclosure of records relating to a surveillance agreement governing the exchange of signals intelligence between the governments of the US, UK, Canada, Australia and New Zealand ("Five Eyes alliance"). Had the information been provided to PI, it could have enabled the exercise of its watchdog function in relation to GCHQ's operations, which conducts wide-scale communications surveillance with significant implications for human rights, not least by enabling it to: (i) review the lawfulness of GCHQ activities and legal advice, including in relation to mass surveillance, (ii) assess the basis on which GCHQ are instructed as to the ethics of their operations, (iii) understand the interaction and compliance of GCHQ with oversight mechanisms, (iv) inform public debate about the information requested, (v) inform its expert submissions on privacy and surveillance issues when engaging with parliamentary and government committees, other international bodies and in litigation.[7]

Both requests were refused. The request to GCHQ was refused without substantiation, claiming rightly that GCHQ has no obligation to comply with FOI requests. PI applied to the European Court of Human Rights claiming violation of Article 10 of the European Convention on Human Rights (ECHR), which protects the right to freedom of expression and information. Developments in UK and ECHR case law led to a settlement between PI and the UK government, but it remains open to PI (and others) to argue that blanket exemptions to FOI laws are unlawful. **Such blanket exemptions are a key question for the Report to address, as arms transfers will often fall within the mandate of national security agencies or other defence departments that can be subject to them.**

[7] For more details see PI's submissions in *Privacy International v United Kingdom*, App no 60646/14, https://privacyinternational.org/legal-action/privacy-international-v-united-kingdom-uk-5ey-foia.

Qualified national security exemptions

Even when a public body is not subject to a blanket exemption from FOI laws, most often countries will also have a qualified national security exemption that requires some application of the public interest test. In practice however, the public interest test is not applied in any granular way, nor are substantiating reasons provided to the requesters.

In 2020, PI with No Tech for Tyrants requested information relating to contracts between the UK's Ministry of Defence (MoD) and Palantir Technologies, a controversial "big data analytics" company that sells software to various government departments around the world – its Gotham software, branded as an "Operating System for Global Decision Making",[8] has been accused of fuelling predictive policing practices.[9] The MoD refused to provide any of the documentation requested, applying the absolute exemption for national security bodies, and the qualified exemption for national security matters: "*The MOD neither confirms nor denies it holds anymore information in addition to the information listed at Annex A under absolute exemption Section 23(5) and qualified exemptions Section 24(2) and Section 26(3). Were the MOD to confirm that information was or was not held, this would alert adversaries to potential services that the MOD could use as part of its defence capabilities. The MOD has a core duty to protect the UK. A Public Interest Test (PIT) has not been conducted for absolute exemption under Section 23(5). A PIT has been conducted for exemptions under Section 24(2) and Section 26(3), and the balance of public interest lay in neither confirming nor denying whether information in scope of the request is or is not held.*"[10] No information was provided as to how the "PIT" had been applied.

Similarly, back in 2016 PI began a quest for transparency and regulation of the use of IMSI catchers by law enforcement in the UK.[11] Starting with two freedom of information requests to the Police and Crime Commissioner for Warwickshire and the Commissioner of Police for the Metropolis (The Metropolitan Police) in October 2016, PI eventually brought two appeals before the Information Rights Tribunal against the UK Information Commissioner (ICO) – which hears appeals against refusals of FOI requests – as it upheld the police forces' decision to withhold information in relation to the use of IMSI catchers. The UK police forces had maintained a strict "neither confirm nor deny" (NCND) policy. In December 2019, the Information Rights Tribunal found in favour of the ICO and dismissed PI's claims. Whilst the decisions of the Tribunal were disappointing, we decided not to appeal them further and have explained our reasons before.[12] Subsequent requests for transparency were not

[8] Palantir, 'Gotham – The Operating System for Global Decision Making', https://www.palantir.com/platforms/gotham/.

[9] Mara Hvistendahl, How the LAPD and Palantir Use Data to Justify Racist Policing (30 January 2021), https://theintercept.com/2021/01/30/lapd-palantir-data-driven-policing/.

[10] Ministry of Defence response to No Tech For Tyrants Freedom of Information Request, 24 June 2020, https://www.whatdotheyknow.com/request/667332/response/1590853/attach/3/FOI2020%200610 9%20Moore%20Interim%20Response%201.pdf?cookie_passthrough=1" \h.

[11] 'IMSI' stands for 'international mobile subscriber identity', a number unique to your SIM card. IMSI catchers are also known as 'Stingrays'.

[12] See further details on the Tribunal's reasoning, PI, 'Information Tribunal Decisions re IMSI Catchers: A loss for transparency and why we will continue the fight through other means' (12 June 2020), https://privacyinternational.org/long-read/3925/information-tribunal-decisions-re-imsi-catchers-loss-transparency-and-why-we-will.

only denied but revealed a lack of clarity regarding the legal framework governing their potential use.[13]

Public order / Prevention of crime / Immigration control exemptions

All countries with access to information laws provide an exemption to disclosure on the grounds of crime prevention or public order. These will also often include or be combined with exemptions for the application of immigration controls. These exemptions are formulated variously as required for the purposes of "public security", "defence and military matters" (EU[14]), "safeguarding national security", "defence", "the prevention or detection of crime", "the operation of the immigration controls" (UK),[15] etc.

In 2019-2022, PI filed a number of freedom of information (FOI) requests with the UK's Department for Work and Pensions (DWP), seeking information on the use by the department of various data analysis technologies to crack down on benefits fraud.[16] The DWP refused to disclose any information on its system for "data matching and data analytics to help identify people who may not have declared their circumstances correctly", applying the "prevention of crime" exemption in a blanket way. A formal complaint to the ICO upheld the DWP's blanket refusal. In light of the potential human rights implications, notably under the International Covenant for Economic, Social and Cultural Rights (ICESCR), of automated benefits systems,[17] this lack of transparency is concerning. Taxpayers and beneficiaries alike are entitled to transparency over the criteria for distribution of social benefits and identification of fraudsters, to ensure proper application of welfare rights. In this instance, much of the information requested could reasonably have been disclosed without any prejudice to current or prospective fraud investigations. This is often the case when security or prevention of crime exemptions are applied.

Requests to the UK's immigration authorities, notably the Home Office, are similarly refused on unsubstantiated grounds of prevention of immigration offences. A request for information regarding an algorithm for prioritisation of immigration enforcement cases, for example, was refused with the simple claim that providing the information would "prove useful to those who might seek to prejudice the operation of an effective immigration

[13] PI, 'Remember those IMSI catchers? UK authorities play hide and seek with use of intrusive surveillance technology' (20 January 2023), https://staging.privacyinternational.org/news-analysis/5206/remember-those-imsi-catchers-uk-authorities-play-hide-and-seek-use-intrusive.
[14] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, Article 4(1).
[15] Freedom of Information Act 2000, ss.24(1), 26(1).
[16] Written evidence submitted by Privacy International to the Public Accounts Committee, https://committees.parliament.uk/writtenevidence/122385/pdf/.
[17] UN General Assembly, "Report of the Special Rapporteur on extreme poverty and human rights," A/74/493, 11 October 2019, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/312/13/PDF/N1931213.pdf?OpenElement.

control".[18] This is a typical claim that prevents all scrutiny of controversial automated triage systems that carry significant implications for the rights of people subject to them.

Commercial interests and intellectual property exemptions

Most countries' FOI laws do not apply to private business entities, and often provide exemptions to disclosure to protect the "commercial interests" of any physical or moral person, and intellectual property rights. These exemptions are often invoked in a way that is over-protective of private commercial interests, failing to fulfil the public interest and presumption in favour of disclosure. They are also often abused by public authorities who rely on them to prevent disclosure of information that is broadly related to a commercial partnership.

Our 2021 request to the UK's Cabinet Office for information regarding the provision of border control software services by Palantir received extensively redacted documents. This included a DPIA, redacted to protect "the strong public interest in allowing public authorities to withhold information which, if disclosed, would reduce its ability, or the ability of third parties, to negotiate or compete in a commercial environment."[19] How the contents of a DPIA threaten commercial interests is unclear. A DPIA is meant to contain information necessary to assess the impact of a data processing operation on data subjects, and hence ought to be fully available for civil society and public scrutiny.

Similarly, a request to Frontex (the European Boarder and Coastguard Agency) for information relating to transfers of surveillance, policing and border control equipment to third countries and the involvement of private entities was refused for it could reveal information "which would undermine the protection of commercial interests of legal persons, including intellectual property."[20] No information was provided, citing the "administrative burden necessary to identify and redact the releasable materials". Hence information that would have been in the public interest to release was not, for commercial interests reasons. This shields significant streams of activity by public authorities from lawful scrutiny.

Other exceptions and limits on the right of access to information

Litigation disclosures

PI has faced similar barriers to access to information during various legal proceedings against intelligence and security services, in particular the UK's Secret Service, Secret Intelligence Service, and GCHQ. The authorities party to the proceedings have invoked

[18] WhatDoTheyKnow, Identify and Prioritise Immigration Cases ("IPIC") Business Rules used by the Home Office (request by Privacy International to Home Office), https://www.whatdotheyknow.com/alaveteli_pro/info_requests/identify_and_prioritise_immigrat_3.

[19] WhatDoTheyKnow, Contracts with Palantir (request by Privacy International to Cabinet Office), https://www.whatdotheyknow.com/request/contracts_with_palantir. For another application of the commercial interests exemption, see PI, 'Amazon Alexa/NHS contract: ICO allows partial disclosure' (27 April 2021), https://privacyinternational.org/news-analysis/4486/amazon-alexanhs-contract-ico-allows-partial-disclosure.

[20] Annex 1 to this submission: Frontex response to Privacy International on 3 July 2020.

exemptions to heavily redact information, as a result extensively prolonging and increasing the cost of legal proceedings.[21]

UN immunity

UN immunities are also sometimes an obstacle to information access. A request to the European Commission for documents related to its collaboration with the UN Office for Counter-Terrorism (OCT) was refused after consultation with the UN OCT as originator of the documents. The reason provided was that "the documents were created by the United Nations and form part of its archives, and are hence inviolable", and that the Contribution Agreement signed with the European Commission states that "any document, information or other material directly related to the implementation of the action and communicated is considered confidential." [22] Hence information that should have been disclosed under national or regional FOI laws is exempted by blanket immunities, preventing any scrutiny of systems deployed under the auspices of the UN.

Costly and time-consuming processes of appeal to supervisory authorities

Exemptions to FOI laws often lead to costly and time-consuming processes of appeal to supervisory authorities. These processes require significant resources, both in terms of time and money, which many individuals and civil society organisations may not have. The need to hire legal counsel, the lengthy wait times for hearings, and the extensive paperwork involved all contribute to the cost. Furthermore, the complexity of these processes can deter individuals and organisations from pursuing their right to information. This not only undermines the principle of transparency but also reinforces the power and information imbalance between public authorities and those seeking information. Therefore, it is crucial to ensure that authorities do not widely use exemptions to FOI laws to prevent disclosure of information and documentation.

Conclusion

Freedom of information laws and policies are essential to effective governance and to accountability of public authorities' decision-making. Through them, journalists, researchers, members of the public, civil society organisations and others are entitled to disclosure of documents held by public authorities or institutions, subject to justifiable exemptions. Yet these exemptions are too widely abused by authorities to prevent disclosure of information that would enhance scrutiny and challenge of their decisions, procedures, operations, relationships, etc. This is particularly true in the context of arms transfers, where national security and commercial interests exemptions are very easily applied and difficult to challenge.

[21] See disclosure and legal proceedings in following cases: PI, 'MI5 ungoverned spaces challenge', https://privacyinternational.org/legal-action/mi5-ungoverned-spaces-challenge; PI, 'Bulk Personal Datasets & Bulk Communications Data challenge', https://privacyinternational.org/legal-action/bulk-personal-datasets-bulk-communications-data-challenge; PI, 'Third Direction challenge', https://privacyinternational.org/legal-action/third-direction-challenge.

[22] Annex 2 to this submission: European Commission response to Privacy International on 28 June 2022.

Recommendations

In particular PI suggests the following main aspects should be covered in the upcoming High Commissioner report:

- Assess states' application of exemptions to access to information laws in the context of arms transfers to ensure compliance with the principle of transparency and the right to information;
- Urge against blanket exemptions for security-related bodies and national security matters as a violation of human rights standards;
- Recommend avenues for appeals and remedies that do not impose excessive financial and procedural burdens on individuals and civil society; and
- Assess the independence and accessibility of access to information oversight mechanisms.