Transparency International Anti-Corruption Helpdesk Answer

Oversight of Intelligence Procurement

Author: Ryan Brunette, tihelpdesk@transparency.org
Reviewer: Caitlin Maslen and Antonio Greco
Date: 12th April 2024

Intelligence procurement can be defined as the acquisition of products that are used to collect and analyse information to support law enforcement and national security functions. These products can be cutting-edge and trust-sensitive, so intelligence procurement often restricts supplier competition by purchasing from sole or preferred providers. Intelligence agencies must also out-manoeuvre the counter-intelligence measures of their targets, which means that intelligence procurement can be secretive. Purchasing from preferred providers and secrecy heighten the risk of corruption and abuse in the process of procuring and using powerful intelligence technologies. This Helpdesk Answer surveys oversight practices that could help to mitigate those risks.

The circumstances justifying departures from open competition and transparency should be clearly specified, narrowly construed, and then adjudicated on a case-by-case basis by independent oversight authorities. In certain areas, such as intelligence in service to criminal policing, measures for radically expanding transparency have been developed and tested. Some intelligence technologies are so dangerous to both national security and human rights that carefully structured bans are appropriate and increasingly applied in practice. These are just some of the oversight practices emerging in a rapidly evolving procurement domain with profound implications for privacy, democracy and safety.

Query

Provide an overview of accountability and oversight mechanisms of procurement processes for the acquisition of goods and services to be used for intelligence purposes.

Main points

- Intelligence procurement often involves secrecy and restriction of competition, which carries risks of corruption and abuse.
- The sphere of legitimate secrecy and circumstances justifying restriction of competition should be construed narrowly and approved by an independent authority.
- In relation to criminal intelligence, there is scope for dramatic expansion of transparency and for representative legislatures to play a role in approving procurements.
- In security intelligence, where secrecy and restriction of competition may be more justified, similar processes of authorisation can proceed through independent expert oversight bodies.
- There is significant movement towards bans and similar restrictions on the purchase of intelligence products.

Contents

1. Background

Intelligence is the process of gathering, analysing, and employing information to support law enforcement and national security objectives. Criminal and security intelligence agencies utilise increasingly sophisticated intelligence technologies, including biometric, drone, web scraping, data interception and predictive analytic systems, to perform this work. These intelligence technologies must ordinarily be procured from external suppliers, such as other intelligence agencies, private firms, and foreign contractors. Generally, public procurement ought to proceed according to norms of open competitive tendering and transparency, but two aspects of intelligence procurement interfere with the application of those norms. First, intelligence goods and services are often innovative, patented and trust-sensitive, which can justify deviation from open competitive tendering in favour of direct approaches to sole or preferred suppliers. Second, if the specific products acquired in the course of intelligence procurement become known more widely, then intelligence targets, which can include criminals, terrorists and hostile foreign powers, can more easily evade scrutiny. The task of mitigating such counterintelligence vulnerabilities and averting threats can justify secrecy.

This relaxation of standard safeguards increases the risk of corruption in intelligence procurement. A case in point is Kyle Foggo, Executive Director of the Central Intelligence Agency (CIA), sentenced for procurement fraud in 2009. Arguing that he needed to work with people he could trust, he steered multiple contracts to a close personal friend, and was rewarded with lavish holidays and a promise of future employment (Born and Wills 2012: 154). In the recent state capture scandal in South Africa, claims of security sensitivity were used to justify removing the State Security Agency (SSA) from ordinary financial controls, to block scrutiny from oversight authorities, and to facilitate procurement practices resulting in the disappearance of the equivalent of hundreds of millions of dollars (Zondo 2022).

A related risk in situations of limited public oversight is the subsequent abuse of the powerful tools that intelligence services have acquired. The South African state capture saga shows how corruption is often tied to wider patterns of abuse. The SSA used its capabilities to shield then-President Jacob Zuma from investigation and criticism, to undermine opposition in his own party, and to spy on activists and journalists (Zondo 2022). In the process, it was an eager participant in a global revolution in surveillance technology, acquiring sophisticated spyware[1] technology widely understood to have profound implications for privacy, freedoms of expression and association, and democracy (Duncan 2018; Richards 2013). In response to the adoption and use of such spyware across Europe, the Council of Europe's Commissioner for Human Rights has argued for member states to "impose a strict moratorium on… export, sale, transfer, and use," pending the development of "a precise, human rights compliant legislative framework for… modern surveillance technology" (Mijatović 2023). In an earlier call for a global pause on sales, United Nations human rights experts asserted, "It is highly dangerous and irresponsible to allow the surveillance technology and trade sector to operate as a human rights-free zone." (OHCHR 2021).

The most prominent example of spyware abuse arises from the Pegasus application developed by the Israeli cyber-intelligence firm, NSO Group Technologies. An attacker can install Pegasus onto a target's devices in a variety of ways, including through the use of zero-click exploits that do not require any action from a device's

1 Spyware, a portmanteau for spying software, is any software application that aims covertly to gather information from a person's computer and to send it to another person.

user. Once installed, Pegasus can be directed to transmit textual, audio, visual, file and location data in real-time from the device back to the attacker. Pegasus can breach encryption protocols in ways that tech giants such as Apple, Google and Meta have found difficult to control (NSO Group Technologies n.d.; Wani 2024). The application demonstrates how private startups like NSO have developed surveillance capabilities previously only available to the world's most powerful states and packaged them into commercially available off-the-shelf products that can be bought by any state and even non-state actors. Investigations into Pegasus have revealed its use in dozens of countries across the world to target journalists, activists, opposition leaders, and even heads of state (Kirchgaessner et al. 2021; Chrisafis et al. 2021).

Pegasus and NSO are only the leading edge of a thriving global industry, reportedly valued at around $ 12 billion in 2022 (Farrow 2022). Researchers have documented over a dozen other commercial spyware vendors operating in 74 countries, democratic and authoritarian, rich and poor (Feldstein and Kot 2023). Growing public outcry has so far generated only nascent regulatory responses (see Maslen 2023). Producer countries have shown little enthusiasm for imposing restrictions on what are highly innovative domestic industries closely integrated into national economic and security objectives. Where trade controls governing conventional arms and dual-use technologies have been expanded to include spyware, vendors have often bypassed these by establishing subsidiaries in countries where those controls are inapplicable or poorly enforced. The governmental and private demand for surveillance technology is so strong, and the costs of entry for new producers low enough, that where companies such as NSO have drawn public scrutiny and limited regulatory action, they may simply lose market share to emerging competitors (Feldstein 2021; Feldstein and Kot 2023). In the absence of effective regulation, civil society has played an important role in detecting and confronting abuses, and it has developed good practices for the work of doing so (Philp 2021; Maslen 2023), but the focus of this Helpdesk Answer is on institutional oversight of intelligence procurement. By the same token, broader issues surrounding the production and use of intelligence products will only be considered here to the extent that oversight of intelligence procurement has a bearing on them.

2. Basics of Intelligence Oversight

Intelligence agencies should be established and operate under tightly circumscribed legal mandates, which may differ according to the type of intelligence agency. While typologies of intelligence agencies are often blurred in the practice of specific countries, Lemieux (2019) distinguishes between criminal intelligence and security intelligence. Criminal intelligence is concerned with collecting information relevant to the prevention and prosecution of interpersonal and communal crimes. The typical location of criminal intelligence is within the local civilian police. Still, national and supranational structures such as the Federal Bureau of Investigations and Interpol can also play a significant role.

In contrast, security intelligence supports the suppression of serious threats to public order, the constitutional regime, and the state. To constrain the potential abuse of security intelligence as a weapon against lawful political activity, security intelligence is ordinarily divided between separate agencies concerned with domestic and foreign menaces. These agencies are often closely related to or housed within the military (see also Brodeur 2010).

Intelligence Oversight Authorities

The role of intelligence oversight is to ensure that the conduct of intelligence agencies complies with those mandates. An initial distinction can be drawn between internal and external oversight. Internal oversight encompasses procedures and authorities contained within intelligence agencies themselves. These should include appropriate professional training and retention of agency staff, effective separation of duties over important processes, a broader framework of organisational control incorporating operationally independent internal finance and compliance offices, and a clear and robust line of command and responsibility leading up to an agency head (CDL-AD 2015: 29-30).

External oversight includes procedures and authorities arising from the broader constitutional and organisational architecture of the state. Four basic types of external intelligence oversight authority are generally replicated for intelligence agencies regardless of whether they are established at national, regional or local levels. Jurisdictions commonly combine these types to provide a system of checks and balances on the activities of agencies with criminal and security intelligence functions (Schierkolk 2018: 20).

The first type of external intelligence oversight authority is the political executive. The political executive is ordinarily responsible for appointing the top directors of intelligence agencies, formulating budgets, asserting policies and directives, authorising the most important agency decisions, facilitating and approving inter-agency cooperation, and reporting to the legislature. These functions should be exercised according to appropriate executive decision-making procedures, framed by principles of rigorous deliberation, collective decision-making, and inter-ministerial checks and balances (Schierkolk 2018: 20-22).

The second type of external oversight authority inheres in legislatures. Legislatures are responsible for facilitating public deliberation, determining the powers of political executives and intelligence agencies, voting on funds available to those agencies, and establishing appropriate checks and balances in overarching statutory frameworks. These statutory frameworks can empower legislatures and opposition parties to be involved in appointing agency directors. They should establish fixed tenure and dismissal procedures for those directors. Political control and operational management of intelligence agencies should be distinguished, with political directives committed to writing and mechanisms for whistleblowing to deal with illicit instructions and activities. Much of the work of legislatures is typically delegated to a committee, where political parties should be proportionally represented. Schierkolk (2018: 27-28) argues that members of these committees should generally not be former employees of intelligence services, and support offices should be properly staffed and resourced.

The first and second types of external oversight authority suffer from two drawbacks. They are tightly embedded in party politics, so the impartiality of their oversight can be brought into question. Politicians and their constituents can also lack the expertise and resources required to engage with the technical complexities of intelligence functions, which means that the extent to which they can exercise effective oversight is often limited.

To address these deficiencies, a third type of external oversight authority covers an assortment of statutorily independent oversight institutions, including expert oversight bodies, ombud institutions, data protection and information commissioners, and state auditors. The leadership of these independent oversight bodies can be subject to statutorily required qualifications and experience. They are appointed by political executives in consultation with opposition party leaders or by legislatures, and they are protected with tenure and dismissal procedures. Expert oversight bodies are highly specialised institutions tasked with exercising day-to-day supervision of intelligence agencies. They can be empowered to pre-emptively authorise intelligence operations, to ensure ongoing compliance with authorisations, and more broadly, to scrutinise and investigate intelligence agencies to ensure they do not act beyond their mandate. A pioneering example is Canada's Security Intelligence Review Committee, which has been a model for 16 out of the European Union's 27 member states.

Ombud institutions often have a mandate extending beyond intelligence oversight specifically, and they are more oriented toward investigating complaints and recommending remediations and reforms. Data protection and information commissioners are responsible for ensuring the appropriate processing of personal information and access to information rights across the state. State auditors conduct external oversight of the finances and, in some cases, the performance of state organisations (Schierkolk 2018: 33-36).

Finally, the fourth type of external oversight authority consists of judiciaries. These often have some powers of ex-ante authorisation, with intelligence agencies required to seek court warrants before engaging in targeted surveillance. However, in intelligence operations, judges often lack specialised expertise and experience, which can be addressed by requiring warrant applications to proceed through high-level panels or by shifting

authorisation power to the independent expert bodies considered above. Courts can engage in ongoing oversight of warranted actions. They also, of course, play an important role in adjudicating legal disputes (Schierkolk 2018: 42-45).

Legitimate Secrecy

A major challenge to effective external oversight arises from the fact that intelligence agencies operate within a sphere of legitimate secrecy. The political ethicist Dennis F. Thompson (1999: 182) argues that this sphere of legitimate secrecy is due to "a fundamental conflict of values that is not readily resolvable and that creates a continuing problem for government secrecy in a democracy." He continues that "the conflict involves this basic dilemma of accountability: democracy requires publicity, but some democratic policies require secrecy." (Thompson 1999: 183) Publicity is essential to the flow of information needed to enhance public debate, make good policy, ensure compliance with law and accountability for abuses, and maintain the people's consent and trust. Still, without secrecy, some democratic processes and policies may not be advanced effectively or at all. Most modern democrats accept the secrecy of the ballot. They would be troubled by the prospect of sensitive negotiations for peace in a war-torn zone breaking down in the full glare of publicity. Intelligence operations ignite the same tension between publicity and secrecy, but often in a more acute form (see also Moynihan 1995; OSJI 2013).

While it is necessary to guard against this argument being pushed too far, intelligence agencies are tasked with investigating what may be dangerous criminals, violent domestic terrorists and hostile foreign powers. The secrecy of intelligence operations is typically justified on the grounds that if the targets, techniques and findings of these operations are prematurely publicised, then the targets could more easily evade law enforcement and national security actions, and they may go on to impose unacceptable costs on innocent victims and society (Manes 2019). But although many would grant the legitimacy of secrecy in at least some such cases (who could confidently assert that secrecy was unjustified if it saved thousands of lives?), it is in the nature of secrecy that the public cannot know its precise extent and content, and intelligence agencies have an incentive to illegitimately expand secrecy to carve out greater operational autonomy, and even freedom from accountability for abuses (Lester 2015: 29-73). The Iran-Contra scandal involved illicit sales of United States arms to Iran and the diversion of a portion of the proceeds to the anti-Sandinista Contra rebels in Nicaragua. The responsible officer justified the operation's secrecy on the view that he was "at a loss as to how we could announce it to the American people and not have the Soviets know about it," but Thompson (2019: 183) concludes that this was beside the point, since "it was not only the Soviets who would have undermined the policy but also many Americans, including a majority in Congress."

It follows that intelligence agencies can err in their assessments of national security demands. Anstis (2021) argues that spyware technologies that emerge from opaque and unregulated markets could be more harmful to national security interests than helpful. There is also vigorous legal debate about whether mass surveillance can ever be justified given its prevalent and often unavoidable harms to privacy, freedom of expression and political association, and democracy (Mitsilegas et al. 2022). However, where precisely to draw the line between transparency and secrecy is difficult to decide in the abstract. Especially in less extreme cases, the question cannot be conclusively resolved without referring to concrete circumstances. So, legal regulations have recourse to basic procedures, principles and safeguards for decision-making. Access to information laws should establish an overarching presumption of transparency. Intelligence agencies should bear the burden of justifying departures from this presumption on a case-by-case basis. These justifications should be carefully weighed against the risks of harm posed by intelligence operations and the strength of the public interest in disclosure. Where an intelligence operation gravely risks or attempts to conceal grand corruption or gross human rights violations, the public interest in disclosure is overwhelming. Even where secrecy is granted, it should always be time-limited, such that when the circumstances justifying secrecy no longer hold, then declassification and open public debate follow (Moynihan 1995; OSJI 2013).

The processes for adjudicating the legitimacy of secrecy may vary according to the type of intelligence agency and its circumstances. The sphere of legitimate secrecy in criminal intelligence is typically smaller than in security intelligence. The targets of criminal intelligence are generally less capable of evading intelligence operations and less dangerous to society. Criminal policing also necessarily pervades and embeds itself within communities. This puts a premium on promoting public accountability, open debate and trust, both to enhance police efficacy and to protect human rights (Manes 2019). As a result, oversight of criminal intelligence is generally more oriented to expanding transparency, with internal, executive, legislative, and independent oversight authorities strongly encouraged to proceed openly (De Angelis, Rosenthal, and Buchner 2016). The equivalent oversight structures for security intelligence are either bound to more stringent confidentiality or face legal constraints on access to state secrets. In this case, bodies tasked with adjudicating the sphere of legitimate secrecy, such as expert oversight bodies, may have to themselves deliberate in secret (DCAF 2010; Born and Wills 2012).

3. Strengthening Oversight of Intelligence Procurement

These distinctions between criminal and security intelligence tend to be recognised by those advancing measures to strengthen oversight of intelligence procurement. Intelligence procurement has only recently emerged as a specific domain of published research and civil society activism, and this section surveys the limited existing literature. The American Civil Liberties Union (ACLU) has led the way in proposing legal mechanisms for constraining the proliferation of intelligence technologies across ordinary policing. Together with allied community organisations, it developed a set of Community Control Over Police Surveillance (CCOPS) Guiding Principles. The first principle asserts that "Surveillance technologies should not be funded, acquired or used without the knowledge of the public or the approval of their elected representatives." (ACLU 2020) The accompanying CCOPS Model Law for City Councils (ACLU 2021) puts intelligence procurement at its centre. It represents the most detailed and comprehensive published proposal now available for overhauling intelligence procurement, and it is presented here as a series of measures that should be creatively adapted to the circumstances of other jurisdictions.

Similar principles and mechanisms to those proposed by the ACLU have been developed for national security intelligence in other countries. Still, these have been less thoroughly elaborated for intelligence procurement in published work and tend to allow more space for secrecy (see OGP 2021). The Geneva Centre for Security Sector Governance's (DCAF) brief on intelligence procurement notes that "procurement by intelligence services is generally regulated by an overarching public procurement law, which provides for some exceptions that accommodate the need to maintain secrecy in the interests of national security." (DCAF 2021) The Open Society Justice Initiative's Tshwane Global Principles on National Security and the Right to Information assert that "national security is one of the weightiest public grounds for restricting information," proceed to strike a careful balance with the demands of transparency, and can be adapted to the circumstances of procurement (OSJI 2013).

Defining the Scope of Intelligence Procurement

The principles and laws proposed by intelligence procurement reformers tend to define the scope of procurement scope broadly. First, they do not confine the definition of intelligence procurement to products obtained by dedicated criminal and security intelligence agencies, but recognise the potential for these products to be obtained and used by a wide variety of other government agencies. The CCOPS Model Law, for instance, refers instead to "municipal entities" and includes within its definition of 'surveillance technology' any "electronic surveillance device, hardware, or software that is capable of collecting… information or communications specifically associated with… any specific individual or group."[2]

2 Section 12(F)

Second, these principles and laws tend to collapse the distinction between purchasing and otherwise obtaining intelligence products. The reason is that intelligence products are often interchangeable between criminal, security and other uses, and are therefore readily transferred from security to criminal and other agencies. In the aftermath of 9/11, the United States federal government identified local police as an important resource in the fight against terrorism. It presided over a surge of funding and transfer of sophisticated intelligence capabilities to local law enforcement. This often occurred without the knowledge and consent of elected councils, and it informed similar processes in other countries (Crump 2016; Feldstein 2021). These processes erode the line between criminal and security intelligence and risk expanding surveillance and secrecy beyond what is justified by the distinct circumstances of each. When a local sheriff's office procures powerful technology for the mass surveillance of mostly law-abiding local communities, an appeal to the urgent demands of national security is not likely to cut it as a justification. So, to mitigate this risk, oversight of intelligence procurement should be designed to scrutinise all processes through which intelligence products are obtained. Oversight authorities should play much the same role regardless of whether intelligence products are bought on the market or received in kind from partner intelligence agencies, and partner intelligence agencies should also be monitored and constrained in the extent to which they can transfer surveillance technologies to others.

With this broad understanding of the scope of intelligence procurement, procurement processes can be divided into pre-acquisition, acquisition, and post-acquisition stages. Pre-acquisition involves identifying needs, researching products and markets, and defining product specifications and contract terms. Acquisition is the process of choosing an acquisition method, selecting suppliers in accordance with this method, and negotiating and finalising contracts. Post-acquisition involves managing performance on contracts, building relationships with suppliers, and reviewing the process to improve outcomes in future (Baily et al. 2022). Each step in a procurement process contains levers which can be used to advance intelligence oversight. The appropriate roles of different types of intelligence oversight authority across procurement processes can be stated in generic terms. Still, advocates of intelligence procurement oversight reform would have to navigate the specific institutional circumstances of their jurisdictions.

Intelligence agencies often operate according to a decentralised organisational model. Granting broad discretion over expenditure to intelligence agents ensures that operations do not follow an obvious pattern and so hostile opponents cannot easily identify targets or predict their actions. However, discretion creates the risk of abuse, so the first task of internal oversight is to assign responsibilities for actioning phases of procurement processes to distinct persons and offices. For example, a distinction can be drawn between the procurement function and the end-user function or between purchase and contract management (DCAF 2021: 17). How this is done should be determined by specific organisational conditions, but appropriate separations of duties must be established to entrench internal checks and balances. The agency head should be responsible for authorising procedures and delegations, approving at least the most important procurements, and establishing a broader framework of organisational control complete with operationally independent finance, compliance and audit offices.

Executive oversight should generally play its traditional role of appointing top directors, formulating budgets, asserting policy, approving procurements with important policy implications, facilitating and approving inter-agency cooperation, and reporting to the legislature. Legislative oversight should also generally play its traditional role of facilitating public deliberation, determining the extent of powers granted to executives and intelligence agencies, voting on funds available to those agencies, and establishing appropriate checks and balances in statutory frameworks. In relation to local criminal intelligence, where resources that can be applied to oversight are scarce, and justifications for secrecy thin, these traditional functions of legislatures can be dramatically expanded toward promoting broad transparency and approving intelligence procurements. In relation to national security intelligence, however, where the resources that can be applied to oversight are relatively abundant, and the justifications for secrecy are often stronger, the powers of expert oversight bodies can be expanded to include monitoring and approvals at various points in intelligence procurement processes.

Pre-Acquisition

The ACLU's CCOPS Model Law declares in its preamble that "it is essential to have an informed public debate as early as possible about decisions related to surveillance technology" (ACLU 2021). In the local policing context, the Model Law aims to radically expand this realm of public debate. In the pre-acquisition stage, a municipal entity will generally identify a need, research products and markets, and define product specifications and contract terms. The CCOPS Model Law goes a step further by requiring this pre-acquisition research and development to be formalised in a Surveillance Impact Report and a Surveillance Use Policy.[3] The Surveillance Impact Report is written, publicly released, and legally enforceable. It describes the surveillance technology, how it works, the purposes for which it will be put, the factors determining its deployment to specific areas, and its fiscal costs. The Report proceeds to make an assessment of any potential adverse impacts on civil and political rights and what measures will be taken to mitigate these.[4]

The Surveillance Use Policy continues to embed the findings of the Report into legal and procedural rules. It governs how each use of the surveillance technology is to be authorised and what potential uses are expressly prohibited. It regulates what data may be collected, how inadvertent collection and retention of data will be minimised, and under what circumstances data will be analysed and reviewed. It also contains safeguards against unauthorised access to data and establishes procedures for limiting retention beyond the purposes for which data is required. The Policy addresses procedures for data sharing, demands for access to data, public complaints, and auditing and oversight of compliance.[5]

Where multiple municipal entities plan to use the surveillance technology, the CCOPS Model Law requires the identification of a lead municipal entity responsible for ensuring compliance.[6] This municipal entity must give public notice, publish its Surveillance Impact Report and Surveillance Use Policy, and provide interested persons with a fair and adequate opportunity to respond before moving to acquisition.[7] The Law recognises that the general public may not be immediately equipped to evaluate complex surveillance technologies, and so it establishes a Community Advisory Committee on Surveillance to help galvanise community interest and consolidate public concerns.[8]

The Model Law directs city councils to approve acquisition only if the benefits outweigh the costs, adequate safeguards of civil and political rights are in place, and discriminatory applications can be ruled out.[9] Should a municipal entity acquire or use surveillance technology without the approval of the city council, then affected persons may approach a court for relief, the prevailing litigant will be awarded costs, and violators will be guilty of a misdemeanour and fined.[10]

These provisions aim to make intelligence procurement transparent, facilitate public debate and input, establish a check through council pre-authorisation of acquisitions, and open access for injured parties to the courts. By frontloading intelligence procurement regulation in the pre-acquisition phase, the CCOPS Model Law limits the potential for procured intelligence products to establish capabilities and practices that exceed existing legal mandates. It also ensures that appropriate safeguards are considered and entrenched before new capabilities come into operation. Proposals have been made for the United States federal and state governments to require CCOPS-like procedures in exchange for federal and state funding and transfer of surveillance technologies (Crump 2016: 1655-1660), but the development of such federal and state conditionalities on transfers appears under-developed.

3 Section 2(A)
4 Section 2(B)
5 Section 2(C)
6 Section 4
7 Section 1(A)
8 Section 8
9 Section 5
10 Section 9

In the domain of security intelligence, advocates for enhanced oversight have tended to respect the distinctions between criminal and security intelligence discussed above. While promoting expanded transparency over security intelligence procurement, they recognise either the ethical or political limitations of advocating for the maximal transparency proposed by the CCOPS Model Law. The Tshwane Principles on National Security and the Right to Information were developed by the Open Society Justice Initiative in collaboration with 22 civil rights and academic centres from across the world. They acknowledge the need for secrecy in certain intelligence operations but require that any government agency seeking to limit information disclosure should demonstrate that the restriction is prescribed by law, necessary in a democratic society, and needed to protect a legitimate national security interest (OSJI 2013). What this involves is a careful process of weighing real and identifiable risks of significant harm to security interests against the overall public interest in transparency. The Principles assert that the law should establish safeguards against abuse, ensure scrutiny of the validity of any restriction by an independent oversight authority, and the possibility of review by the courts.[11]

The Tshwane Principles do not contemplate the specificities of intelligence procurement, but in light of the Tshwane Principles, ACLU's CCOPS Model Law can be adapted to the context of security intelligence procurement context. The Open Government Partnership (OGP) argues for the preparation of impact assessments for intelligence procurements and a presumption of openness in the proceedings of intelligence oversight authorities, but it allows for security intelligence agencies to make a case for secrecy and for oversight authorities to approve if this is deemed to be legitimate (OGP 2021). DCAF advises similarly, arguing for maximum transparency in intelligence procurement but allowing an independent oversight authority to approve secrecy in specific circumstances (DCAF 2021). The CCOPS Model Law's more detailed provisions for impact reports, use policies, and acquisition authorisation are relevant here. The greater need for secrecy and added complexity of security intelligence procurement would tend to mean that an independent expert oversight body would be best placed to determine the sphere of legitimate secrecy, scrutinise impact reports and use policies, and authorise acquisition. The executive would have primary responsibility for setting direction and ensuring implementation. The legislature would be required to set the legislative framework and exercise general oversight of both the executive and the independent expert oversight body. The judiciary would be responsible for settling disputes and review.

A final element of pre-acquisition oversight and control is the possibility of outright bans on certain intelligence products. In the wake of the Snowden revelations, the European Court of Human Rights has engaged extensively with the legality of bulk surveillance, ultimately allowing it in appropriately regulated circumstances (ECHR 2021). Activists have campaigned with some success for bans on facial recognition technology at the local government level in the United States and elsewhere (Dauvergne 2022). President Biden has signed an executive order prohibiting the federal government from making operational use of commercial spyware where there is credible information that such use poses risks to the security of the United States government or risks of improper use by a foreign government or person. These risks are described broadly enough to encompass all commercial spyware that has been used in the past to violate human rights (Biden 2023). The European Union is in intensive deliberations regarding its own spyware ban. The United States federal government's ban on communications and surveillance technologies from a series of Chinese tech giants follows a different logic, that of geopolitical and economic competition (Miller 2022). Nevertheless, blacklisting certain companies and countries could also be justified on human rights terms (Born and Wills 2012).

Acquisition

The role of independent oversight authorities can extend to monitoring intelligence agencies' choice of acquisition methods. The United Nations Commission on International Trade Law (UNCITRAL) Model Law on Public Procurement establishes a global standard for types of acquisition methods and the circumstances

11 Principle 3

governing their selection (UNCITRAL 2011). It stipulates that procuring entities should generally conduct procurement by means of open competitive tendering.[12] This default of open competition in procurement presents a significant defence against corruption and abuse. It ensures a measure of transparency, requires adjudication of competition according to fair and objective criteria, and leverages the market and the interests of competing bidders as a check on official discretion.

Nevertheless, the Model Law also provides for specific circumstances under which restriction of open competition can be justified. Where the product sought is so complex or specialised that only a limited number of suppliers or a sole supplier can provide it, then competition can be constrained accordingly.[13] If the time and cost required to solicit and evaluate tenders would be disproportionate to the value of the product, or if an emergency justifies immediate approach to a supplier, then this would also justify the restriction.[14] The Model Law provides reasonable allowance for situations where products must be supplemented by additional supplies from the same provider.[15] The Law also allows for procuring entities to approach specific suppliers where "the use of any other method of procurement is not appropriate for the protection of essential security interests of the State."[16]

However, the Model Law does not recognise any blanket exception allowing all intelligence procurement to depart from open competition. Good practice in this space requires that intelligence procurement operates according to the general rules of procurement, with deviations from open competition justified in relation to the circumstances provided for within these rules. The ACLU's CCOPS Model Law, for instance, does not consider purchasing methods, effectively assuming that surveillance technology will be obtained according to general procurement procedures. The OGP (2021) guidance similarly affirms that intelligence procurement processes should continue through an open process unless a restriction is justified before an independent oversight authority. Likewise, the DCAF (2021) brief on intelligence procurement notes that internal procurement procedures should follow general principles of public procurement, that they should not arbitrarily discriminate between or limit the participation of suppliers, but that special procedures and secrecy may be applied in specific circumstances. In Poland, for instance, the country's Public Procurement Act applies across the intelligence community. Most purchases by Poland's intelligence agencies do not raise issues of national security, so they proceed in terms of the ordinary rules of the Act. However, intelligence agencies can formally justify exceptions of specific security intelligence procurements from the Act, which, if successful, means that the procurement in question will proceed through special and secret agency processes.

These procedures for deviation from open competitive tendering could be streamlined with those proposed by the CCOPS Model Law. In the case of criminal intelligence, this would mean that the entity promoting the acquisition of intelligence products would be required to table not only an Impact Report and a Use Policy but also an Acquisition Plan laying out the case for pursuing a specific method. These could collectively be presented for public comment, open deliberation, and authorisation by the relevant legislature. Security intelligence procurement could proceed similarly but with appropriate restrictions on transparency approved by an independent expert oversight body.

Advocates pursuing these options should be careful to ensure that these oversight procedures do not become an excessive bottleneck in legitimate procurement processes. This risk is especially relevant to emergency situations, where fast-track or post-hoc procedures ought to be considered.

Once an acquisition method is chosen, the next step is to select suppliers. In open and restricted competition methods, criteria for evaluation should be fair, objective, and quantifiable. The decision to award contracts to

12 Article 28
13 Article 29.1.(a) and 30.5.(a)
14 Article 29.1.(b) and 30.5.(b)
15 Article 30.5.(c)
16 Article 30.5.(d)

specific suppliers should be recommended by a committee separate and independent from officials involved in earlier stages of the process, and at least for the most important procurements authorised by the head of the relevant intelligence agency. Where an allowance is made at this point for selection to depart from the lowest cost or highest score rule, then this should be reasoned on objective grounds and submitted to the appropriate oversight authority.

The UNCITRAL Model Law addresses a wide range of particulars regarding contract negotiation and finalisation. Notably, the CCOPS Model Law prohibits contractual agreements that conflict with the provisions of the Law.[17] This extends to contractual agreements that violate use policies or that include non-disclosure clauses. The same should apply to security intelligence procurement, where legal prescripts should prohibit contractual agreements that violate use policies, and non-disclosure clauses that interfere with oversight processes should not be permitted.

Post-Acquisition

Post-acquisition commences with contract management, supplier relationship management and procurement performance review. In relation to criminal intelligence, the CCOPS Model Law again contains relevant provisions. It requires, within 120 days of the Act's effective date, a review of pre-existing uses of surveillance technology. Each and every pre-existing technology is to go through the same approval process as required for new surveillance technologies. Where this approval process is not completed within 180 days, then surveillance using that technology is to cease.[18] If the relevant municipal entity plans to use an approved surveillance technology in a new way, then the same process of approval is to be followed, constituting a check on the proliferation of unapproved surveillance applications.[19]

The CCOPS Model Law requires the relevant municipal entity to develop annual surveillance reports for every surveillance technology used. These are to outline how surveillance technology has been used, how often data was shared with or received from external persons or entities, where the technology was deployed geographically, a summary of complaints or concerns raised about the technology, the results of audits and information about violations of use policy, an analysis of discriminatory impacts, and the total costs of use.[20] Where use of the surveillance technology does not meet the standard of approval laid down in the Model Law – for example, if its benefits do not outweigh its costs, if safeguards of civil and political rights have proven inadequate, or if discriminatory and disparate impacts are shown – then the City Council is directed to discontinue use of the surveillance technology, or to modify the relevant Use Policy to remedy the defects.[21] The Model Law continues to require city councils to prepare annual public reports on the implementation of the Act.[22] The Law includes rights to approach the courts for remedies, makes it a misdemeanour punishable by fine to violate any of its provisions, and contains protections for whistleblowers.[23]

These same mechanisms are feasible, with appropriate adjustments, in the security intelligence domain. Legislation can require reviews of pre-existing uses of surveillance technology, re-authorisation of these uses, and new procedures for authorising changes in use policies. Legislation can also provide for periodic reports on the implementation of use policies and legal mechanisms for correcting deficiencies and abuses. The higher threshold for secrecy in the security intelligence space will likely require these functions to be performed by independent expert oversight bodies, appropriately supported by the executive, legislated by the legislature, and reviewed by the courts. In the space of automated decision-making and artificial intelligence systems, Access Now has called for the European Union to require member states to conduct

17 Section 10
18 Section 3
19 Section 1(A)(3)
20 Section 6(A)
21 Section 6(C)
22 Section 7
23 Section 9

mandatory human rights impact assessments and establish public registers. These public registers are to disclose the use, purpose and developers of such systems. The public registers are also to incorporate mechanisms to notify and coordinate relevant authorities, including national centres of expertise composed of regulators, civil society, and academia, and they must be tasked with monitoring, researching and providing advice to government and industry (Access Now 2020). These more far-reaching proposals can be adapted to the security intelligence space. Still, advocates would need to navigate the national security interests and justifications likely to push back against and moderate them.

At this point, however, post-acquisition safeguards fade out from the procurement of intelligence products into general intelligence regulation and oversight. This is a complex regulatory domain beyond the scope of the current study. DCAF's compendiums of guiding principles and toolkits for intelligence oversight are important for this work (DCAF 2010; Born and Wills 2012). Dycus et al. (2020) provide a comprehensive discussion of the contemporary legal situation in the United States. Wetzling and Vieth (2018) also provide a reasonably up-to-date compendium of oversight innovations from Europe, North America, and Australasia. They deal with the intelligence cycle across strategic planning, application for surveillance operations, authorisation, collection and filtering, data processing, analysis, review and evaluation, and reporting.

Consideration should also be given to a more recent movement requiring that persons subject to surveillance be notified after the purpose of that surveillance expires. To this effect, a bipartisan Government Surveillance Transparency Bill was introduced into the United States Senate in 2022 (Wyden et al 2022). In 2021, in the aftermath of the findings of its judicial inquiry into state capture, South Africa's Constitutional Court struck down the country's communication interception law on the grounds that it did not provide for notification to surveillance subjects. The Court continued to require special safeguards against the surveillance of practicing lawyers and journalists to protect their professional obligation to maintain confidentiality of their clients and sources (CCSA 2021).

CCOPS Model Law Implementation Outcomes

The movement behind the CCOPS Model Law has probably gone the furthest in subjecting intelligence procurement to transparency and democratic oversight. The justifications for secrecy in community policing are weaker than in security intelligence, and so local government has proven to be something of a soft underbelly of the American surveillance state. The path for the CCOPS movement has likely also been eased by the party-political profile of urban government in the United States, with the Democratic Party generally more attuned to demands for checking police powers. The strategic terrain will, of course, differ across countries, but reform tacticians are generally well-advised to target advocacy to those points in national intelligence systems where they will be most likely to make headway.

Several local governments have enacted versions of the CCOPS model law, but they have often been weakened in the course of passage. City police are powerful actors in local politics, and they have succeeded in significantly redrawing CCOPS laws to suit their interests. For instance, New York City's Public Oversight of Surveillance Technology Act of 2020 narrows the definition of surveillance technology to exclude parking ticket devices and cameras installed to monitor and protect the integrity of city infrastructure. It requires surveillance technology impact and use policies to be published for public comment. Nevertheless, its provisions are vague enough to enable the New York Police Department (NYPD) to release impact and use policies for general categories such as "situational awareness cameras," obfuscating distinctions between different camera-equipped technologies with diverse capabilities and made by a variety of companies. The NYPD has often been accused of not following the Act, but the New York City Council has little power to block new surveillance purchases, rewrite NYPD use policies, or prosecute transgressions of the Act (NYCC 2020; McDonough 2023).

There have been some studies on the implementation of the more extensive laws passed in Seattle, Oakland, Berkeley, and San Francisco (Southerland 2023). In all four cities, officials have had to reveal to the public

aspects of their surveillance technologies and how these are used. This has heightened public awareness and mobilisation around intelligence technology concerns. In Seattle, it emerged, through the operations of its CCOPS law, that an individual detective had acquired facial recognition technology on their own. The detective was reprimanded, and the City Council subsequently enacted a county-wide ban on that technology. During a similar process, Oakland banned predictive policing and biometric surveillance technology in 2021. Surveillance in these cities has also been curtailed in more detailed ways, an example being Oakland residents' successful effort to block the rollout of cameras across its Chinatown district.

Implementation of CCOPS-style laws has, however, also run up against limits in these cities. None of the cities included provisions barring the use of technologies without council approval. They also never criminalised violations of their laws. Oversight bodies have remained under-resourced in relation to the often-sophisticated capabilities of the police. These factors have resulted in persistent non-compliance with the laws. Oakland's relatively high crime rate and inequality have made it a particular flashpoint, where police have often simply defied reporting requirements. Levels of community engagement with CCOPS processes in all four cities have been limited. Southerland (2023) also raises the concern that without sufficient political will and capacity, councils seem often to have rubber stamped police applications. He argues that CCOPS laws, improperly applied, can merely legitimise problematic intelligence practices.

The record of implementation is, therefore, mixed. Southerland (2023) finds that CCOPS-style laws providing for representative community advisory bodies have been more successful at encouraging community engagement. He argues that the laws should be amended to provide these advisory bodies with more power and resources to investigate transgressions and to veto council decisions. He also suggests that the legislative check on surveillance technology purchases can be strengthened by putting a presumption against introducing new surveillance technology into law and requiring stronger justifications to overcome this presumption.

4. The Use of Procurement to Regulate the Intelligence Technology Market

This Helpdesk Answer is concerned with enhancing oversight to prevent corruption and abuse within intelligence procurement. However, enhanced oversight over intelligence procurement could bring wider benefits in strengthening the regulation of intelligence technology markets. The role of public procurement in advancing secondary (also known as horizontal) policy objectives is well-established. Beyond the primary objective of obtaining a product, public procurement frameworks can shape markets in such a way as to promote broader economic, social, and environmental (or, indeed, anti-corruption) goals. Given the size of procurement markets and the fact that the government is typically the largest purchaser in national economies (OECD 2023), robust procurement frameworks for intelligence sector products could potentially drive positive changes in the production and use of intelligence technology.

Anstis (2021) has made the case for introducing secondary policy goals into the procurement of intelligence technology. She argues that the market, especially for off-the-shelf spyware products, is so opaque and unregulated that intelligence agencies who purchase from it face the risk of undisclosed vulnerabilities that opponents can exploit. This means that these intelligence products are not simply a threat to citizens' civic rights but they also create operational and national security risks for the state. On these grounds, Anstis calls for governments to insert governance and transparency conditions into their contracts with purveyors of intelligence technology.

The conditions she proposes range widely. She argues that contractors could be compelled to disclose their ownership structure, relationships with their host state, and the number of sales they have made of specific intelligence products. Contractors could be required to certify that sales are only made to allied governments, that products comply with human rights law, and to establish compliance processes within their operations.

Contracts could also stipulate that contractors submit themselves to court proceedings and establish a domestic company presence to address any court jurisdiction issues.

Requiring contract conditions is only one way to assert secondary policy goals in procurement processes. Arrowsmith (2010) provides a comprehensive survey of other available measures, including outright bans, more limited restrictions on purchases of products with certain qualities, exclusion of companies that don't meet certain standards, and preferring companies that meet standards in invitations to tender and points scoring. Biden's executive order "banning" the purchase of certain spyware is best understood as a more sophisticated attempt to use secondary measures in procurement to shape the commercial spyware market. The executive order excludes from the world's largest potential buyer companies that sell spyware products that use data in ways that are not authorised by the end-user, that have disclosed or intend to disclose non-public information about the United States government, or that are under the control of a foreign government that conducts espionage against the United States. The executive order also excludes companies that have sold spyware products that a foreign government or person has used to collect information about civil society actors in ways that violate citizen rights or have sold spyware products to governments that engage in gross human rights violations (Biden 2023).

Using national procurement rules to shape a global market for intelligence products faces obvious collective action problems. Still, each step by a national government begins to bifurcate the market between legitimate and illicit vendors. The restrictions imposed by the United States, along with the looming efforts of the European Union, have already produced anxieties within the global digital surveillance industry. James Lewis, a senior vice president at the Center for Strategic and International Studies, notes, "Some of them have told me that they're not sure they're going to be able to stay in business at all" (in Kagubare 2023).

References

Access Now. 2020. Trust and excellence - the EU is missing the mark again on AI and human rights.

ACLU (American Civil Liberties Union). 2020. Community Control Over Police Surveillance Guiding Principles.

ACLU (American Civil Liberties Union). 2021. Community Control Over Police Surveillance (CCOPS) Model Law.

Anstis, Siena. 2021. Government procurement law and hacking technology: The role of public contracting in regulating an invisible market. Computer Law & Security Review, 41, pp.1-16.

Arrowsmith, Sue. 2010. Horizontal Policies in Public Procurement: A Taxonomy. Journal of Public Procurement, 10(2), pp.149-186.

Baily, Peter, David Farmer, Barry Crocker, and David Jessop. 2022. Procurement Principles and Management in the Digital Age, 12th Edition. London: Pearson Education Limited.

Biden, Joseph R. 2023. Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security.

Born, Hans and Aidan Wills, eds. 2012. Overseeing Intelligence Services: A Toolkit. Geneva: DCAF.

Brodeur, Jean-Paul. 2010. The Policing Web. London: Oxford University Press.

Chrisafis, Angelique, Dan Sabbagh, Stephanie Kirschgaessner, and Michael Safi. 2021. Emmanuel Macron identified in leaked Pegasus project data. The Guardian.

CCSA (Constitutional Court of South Africa). 2021. AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others.

CDL-AD (European Commission for Democracy Through Law, the Venice Commission). 2015. Report on the Democratic Oversight of Signals Intelligence Agencies. Adopted by the Venice Commission at its 102nd Plenary Session.

Crump, Catherine. 2016. Surveillance Policy Making by Procurement. Washington Law Review, 91(4), pp.1595-1662.

Dauvergne, Peter. 2022. Identified, Tracked, and Profiled. The Politics of Resisting Facial Recognition Technology. Northampton, MA: Edward Elgar Publishing.

DCAF (Geneva Centre for Security Sector Governance). 2010. Compilation of Good Practices for Intelligence Agencies and their Oversight. Report to the UN Human Rights Council by the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism.

DCAF (the Geneva Centre for Security Sector Governance). 2021. Thematic Brief: Intelligence Procurement.

De Angelis, Joseph, Richard Rosenthal, and Brian Buchner. 2016. Civilian Oversight of Law Enforcement: Assessing the Evidence. OJP Diagnostic Center and the National Association for Civilian Oversight of Law Enforcement.

Duncan, Jane. 2018. Stopping the Spies: Constructing and Resisting the Surveillance State in South Africa. Johannesburg: Wits University Press.

Dycus, Stephen, William C. Banks, Peter Raven-Hansen, and Stephen I. Vladeck. 2020. National Security Law. Frederick, MD: Aspen Publishing.

ECHR (European Court of Human Rights). 2021. Case of Big Brother Watch and Others v. the United Kingdom.

Farrow, Ronan. 2022. How Democracies Spy on their Citizens. New Yorker.

Feldstein, Steven. 2021. The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance. New York: Oxford University Press.

Feldstein, Steven and Brian (Chun Hey) Kot. 2023. Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses. Carnegie Endowment for International Peace.

Kirchgaessner, Stephanie, Paul Lewis, David Pegg, Sam Cutler, Nina Lakhani, and Michael Safi. 2021. Revealed: leak uncovers global abuse of cyber-surveillance weapon. The Guardian.

Lemieux, Frederic. 2019. Intelligence and State Surveillance in Modern Societies: An International Perspective. London: Emerald Publishing Limited.

Lester, Genevieve. 2015. When Should State Secrets Stay Secret? Accountability, Democratic Governance, and Intelligence. New York: Cambridge University Press.

Manes, Jonathan. 2019. Secrecy and Evasion in Police Surveillance Technology. Berkeley Technology Law Journal, 34(2), pp.503-566.

Maslen, Caitlin. 2023. The implications of spyware and surveillance technology for anti-corruption activists. U4 Helpdesk Answer.

McDonough, Annie. 2023. NYPD may be violating police surveillance transparency law. City & State New York.

Mijatović, Dunja. 2023. Highly intrusive spyware threatens the essence of human rights. European Commissioner for Human Rights Comments.

Miller, Christopher. 2022. Chip War: The Fight for the World's Most Critical Technology. New York: Scribner.

Mitsilegas, Valsamis, Elspeth Guild, Elif Kuskonmaz, and Niovi Vavoula. 2022. Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks. European Law Journal. 109(1-2), pp. 176-211.

Moynihan, Daniel Patrick. 1995. Commission on Protecting and Reducing Government Secrecy.

New York City Council. 2020. Public Oversight of Surveillance Technology Act.

NSO Group Technologies. No date. Pegasus – Product Description.

OGP (Open Government Partnership). 2021. Innovations in Democratic Oversight of Surveillance from OGP Members.

OHCHR (United Nations Office of the High Commissioner on Human Rights). 2021. Spyware scandal: UN experts call for moratorium on sale of 'life threatening' surveillance tech.

Open Society Justice Initiative. 2013. Global Principles on National Security and the Right to Information ("The Tshwane Principles").

OECD (Organization for Economic Cooperation and Development). 2023. Government at a Glance.

Philp, Rowan. 2021. Tips to Uncover the Spy Tech Your Government Buys. Global Investigative Journalism Network.

Richards, Neil M. 2013. The dangers of surveillance. Harvard Law Review, 126(7), pp. 1934-1965.

Silberman, Michael. 2024. Policing Pegasus: The Promise of U.S. Litigation for Commercial Spyware Accountability. Georgetown Law Technology Review, 8, pp.245-286.

Southerland, Vincent M. 2023. The Master's Tools and a Mission: Using Community Control and Oversight Laws to Resist and Abolish Police Surveillance Technologies. UCLA Law Review, 70(2), pp.1-90.

Thompson, Dennis F. 1999. Democratic Secrecy. Political Science Quarterly, 114(2), pp.181-193.

UNCITRAL (United Nations Commission on International Trade Law). 2011. Model Law on Public Procurement.

Wani, Maknoon. 2024. Israel's Spy-Tech Industry Is a Global Threat to Democracy. Jacobin.

Wetzling, Thorsten and Killian Vieth. 2018. Upping the Ante on Bulk Surveillance: An International Compendium of Good Legal Safeguards and Oversight Innovations. Heinrich Böll Stiftung.

Wyden, Ron, Steve Daines, Mike Lee, and Cory Booker. 2022. Government Surveillance Transparency Act of 2022.

Zondo, Raymond. 2022. Report of the Judicial Commission of Inquiry into Allegations of State Capture, Corruption and Fraud in the Public Sector: Part V. Volume 1: State Security Agency and Crime Intelligence.

TRANSPARENCY INTERNATIONAL
the global coalition against corruption

"Anti-Corruption Helpdesk Answers provide practitioners around the world with rapid on-demand briefings on corruption. Drawing on publicly available information, the briefings present an overview of a particular issue and do not necessarily reflect Transparency International's official position."

Transparency International
International Secretariat
Alt-Moabit 96
10559 Berlin
Germany

Phone: +49 - 30 - 34 38 200
Fax: +49 - 30 - 34 70 39 12

tihelpdesk@transparency.org
www.transparency.org

transparency.org/en/blog
facebook.com/transparencyinternational
twitter.com/anticorruption

Transparency International chapters can use the Helpdesk free.
Email us at ***tihelpdesk@transparency.org***