# Innovations in Democratic Oversight of Surveillance from Open Government Partnership Members

**Overview**

- Limitations on surveillance are necessary for a prosperous society.
- Citizen oversight is an essential part of that function.
- Citizen oversight requires investment in (a) transparency and disclosure of activities and impacts; (b) public access to formal oversight mechanisms; (c) adequate safeguards for private sector activity; and (d) records management.

Safeguards to protect privacy, democracy, and free expression need to keep up with evolving technologies, including surveillance technologies. Protecting from abuses of surveillance by the executive requires legislative and judicial counterweight. Just as importantly, however, the public oversight of the purchase, use, and disposal of surveillance technologies (and the information they produce) is necessary to ensure that interference of private communications is legal and proportionate.

This document outlines steps governments can take to improve public oversight of surveillance technologies. It is based on the experiences and standards across a range of OGP countries, including a number of important commitments undertaken in OGP action plans. It aims to inspire new commitments and reforms to enhance public oversight in this critical policy area.

## WHY LIMIT SURVEILLANCE?

Limits on surveillance are essential for the protection of privacy. Privacy is a good in its own right, and is essential to the functioning of democratic societies.

- **Personal reasons:** Individuals and families need to be able to express themselves and interact in private spaces, virtual and real.
- **Protect property and personal safety:** Sharing of data, especially location data, can lead to dangerous intimidation, violence, or harassment.
- **Protecting speech and right to dissent:** Maintaining privacy is essential for free thought, in turn essential for free expression, which is the cornerstone of democracy and human rights.
- **Commercial standards and harmonization:** Companies working across borders, including in trade in online goods and services, seek regulatory harmonization to ensure that products are compatible with the market rules in a variety of countries, including rules around data protection. In addition, they have a reasonable expectation of fair competition, which includes protection from commercial espionage.

Beyond the instrumental arguments for limits on surveillance, there is a strong normative basis for safeguards. International law limits the extent of surveillance and increasingly has become the norm under national and regional law.

- The Necessary & Proportionate Principles provide guidance on how human rights law applies to digital surveillance to ensure that surveillance is only justified when prescribed by law, when it is necessary to achieve a legitimate aim, and proportionate to the aim pursued.
- The Tshwane Principles, developed collaboratively by civil society, government, and private sector give guidance on how the law can establish safeguards to national security surveillance.
- The right to privacy and the right to freedom of expression without interference are both human rights enshrined in the Universal Declaration of Human Rights.
- Increasingly, governments around the world are enacting national privacy and data protection laws.

## SURVEILLANCE IN THE OPEN GOVERNMENT PARTNERSHIP

Citizen oversight has been central to the Open Government Partnership (OGP) since its earliest days. In fact, Ambassador John Kerry, first acknowledged the Snowden leaks, which uncovered the extent of US surveillance, while speaking at the OGP London Summit in 2013. It was around this time that a large group of civil society organizations working on OGP in their respective countries urged the international community, and national members of OGP, to review their national laws and to commit to greater transparency in matters related to surveillance technology.

Since early efforts at the international level, several countries have adopted such commitments in their OGP action plans.

## POTENTIAL REFORMS

Below are a set of reforms to enhance public oversight and democratic controls on interventions of private communications. Recommendations are based on actions made by OGP members in these or tangentially related topics.

### Transparency and disclosure of activities and impacts

- **Impact assessment:** Require ministries, departments and agencies executing a program or procuring contracts and granting to carry out privacy risk screening and impact assessment.
    - **Tools:** There are three increasingly common types of impact assessment used which have overlapping functions. (See box, “Privacy Impact Assessments” for examples.)
        - *Privacy impact assessment* - to establish specific effects on personal data and information;
        - *Algorithmic impact assessment* - which might go beyond personal impacts to collective impacts, such as effects on democracy or discrimination, but which is limited to data processing.
        - *Human rights impact assessment* - which may include right to privacy among other core rights such as right to seek and share information.

## Privacy Impact Assessments across OGP

Several OGP members have made strides in impact assessment which can serve as an input and information gathering process to inform oversight of activities. Impact assessments are often participatory, gathering insights from experts and affected communities during preparation of the document. In addition, impact assessments can help with after-the-fact accountability, ensuring that appropriate safeguards were put in place, monitored, and responded to. Three examples follow:

- United States: Improve Transparency of Privacy Programs and Practices. This notable and complete commitment sought to enhance the quality and publicity of privacy impact statements during federal procurement and other federal activities which would affect the processing of personal data. Notably, this covered issues of national security and surveillance.
- Canada: Privacy screening. Canada has introduced a privacy screening tool to raise a red flag or identify the need for legal review in software procurement that would have an impact on personal data.
- European Union: Data Protection Impact Assessment. This tool is required of companies and agencies undertaking data processing as defined by the General Data Protection Regulation (GDPR).

- **Establishing a presumption of openness in administrative procedures**: Require acting officers to make a positive case for secrecy of a decision-making process before an established, independent commission. Exemptions should be narrow, legally-based, and specific. Special attention within the context of surveillance procurement and deployment should minimize claims of confidential business information, trade secrets, and minimize secret law. Dozens of OGP countries have made significant commitments in this area.
- **Establishing a presumption of openness in procurement**: Require acting officers to make a positive case for secrecy before an established, independent commission for procurements meeting a certain threshold. If such cases are not approved, contracting from tender to execution and evaluation should be part of an open contracting procedure. These exemptions should be rare. Australia, which has such a rule, has flagged 2.7% of all national security contracts, a small number, even in an area of activity known for secrecy.
- **Data processing registers:** Establish a public data processing register which allows for public oversight of data processing (usually defined, at a minimum, as "collection, storage, modification, transfer, and disposal.") The GDPR requires all EU member states to publish such registers. France's data protection register is the first such register, although dozens are expected to come online in coming months, even beyond the EU.

## Formal oversight

- **Establish a multistakeholder oversight body:** This body would be composed of officials, permanent staff, and qualified members of the public selected through a transparent process and standards. The mandate may include:
  - Review and recommendation of policy and practices
  - Examination of specific individual actions
  - Receipt of complaints
  - Referral of evidence or cases to public advocates

  Some OGP members have established oversight bodies in other sectors such as public procurement. Ukraine's ProZorro e-procurement system includes DoZorro, a citizen monitoring platform. DoZorro allows citizens to access data, submit feedback and flag irregularities, which are then channeled to the appropriate authority.

- **Establish or enhance a Data Protection Authority:**
  - Data protection authorities would typically have a mandate to carry out the following oversight functions (See box "South Africa and Brazil" below:
    - Ensuring regular, periodic reporting and compliance with transparency requirements (see below) of regulated entities;
    - Fact-finding and investigation for particular harms and reference of findings and recommendations to appropriate judicial authorities. These may be triggered by public requests or initiated directly by the authority;
    - Regular reporting to parliament on surveillance and personal data protection regime.
  - Some authorities would have the following powers:
    - Subpoena powers for documents and testimony (including ability to hold non-compliant individuals in contempt);
    - Ability to initiate independent investigations;
    - Ability to assign fines or other sanctions to regulated entities that are found not to be compliant;
    - Training for individuals, communities, and other levels of government in rights, procedures, and compliance.

## Formal oversight (continued)

- **Surveillance courts**
  - **Establish specialized transparency courts** with a mandate to protect privacy and minimize intrusion according to constitutional and statutory requirements.
  - **Meta-data on personal data requests** - how many agencies made requests, including how many denials, how many appeals, nullifications and confirmation by courts.
  - **Public parliamentary oversight** - require periodic reviews of performance of courts relative to their mandate of privacy protection and civil liberties.

### Georgia: Balancing Security with Disclosure

Following the Rose Revolution in Georgia, the central government gained increasing powers of surveillance. In some cases, this surveillance was used on political and commercial rivals. In response to growing concern, as part of its action plan, Georgia's Supreme Court committed to producing statistics on motions for phone tapping. The Supreme Court went beyond its initial goal of producing quarterly internal statistics; following a request from OGP Forum members, the Supreme Court began making that data public on an annual basis. Continued dialogue between the Supreme Court and civil society groups focused on expanding the metadata to include bulk downloads, disclosure of justification by type of crime, and geographic data. OGP's Independent Reporting Mechanism (IRM) has positively evaluated this commitment both in terms of the quality of implementation and its early results. This success demonstrates how OGP can be used successfully to enable better citizen oversight of surveillance.

- **Whistleblower protection for security staff**
  - Establish a chain of complaints and appeals that allows security staff to file cases of waste, fraud, and abuse in agency actions. Such a chain of complaints would allow whistleblowers to go directly to an ombudsman's office, inspectorates or their equivalent without exhausting the chain of immediate supervisors.
  - In turn, inspectorates, auditors, and ombudsman offices may be required to report such cases in detail to parliamentary oversight committees with appropriate security protocols.
  - Establish a legal right of action for those complaining of whistleblower retaliation.
  - Establish *personal* liability for retaliation by superior officers toward whistleblowers. This would include a range of remedies from restoration and fines, to removal from office and potential criminal charges for egregious cases.

## Formal oversight (continued)

- **Whistleblower protection for private contractors -** Many security and surveillance activities are outsourced to private contractors who do not benefit from the same channels for reporting wrongdoing and employment protection from retaliation. (See box, "United States: Whistleblower Protection" for more.)
- **Private and public interest right of action -** Establish a private right of action for individuals to seek remedy and redress when they have established a material violation of privacy. Where such a right exists, such a right may be enhanced through:
    - Statutory implementation of constitutional *writ of amparo* or the *writ of habeas data* in cases where an individual (natural or legal) or community believes there to be a harm or *potential harm.*
    - The establishment of administrative and judicial courts, which allow for, among other things, challenging decisions issued by the Data Protection Authority**.**
    - Loosening restrictions on standing (to allow for *amicus curiae* filings) and class actions in cases of surveillance and privacy; some statutes may establish "public interest" rights to allow legal persons to seek redress and remedy for harms to the public interest.
    - Establishment of material supports for filers of complaints, such as ombudsmans' offices, removal of court fees for public interest action (including "English rule" court costs), and protections for filers, especially of vulnerable groups.

### United States: Whistleblower Protection

For over four decades, the United States whistleblower protection has evolved. Most saliently, the pertinence of these rules was highlighted in 2019, when a CIA whistleblower's allegations led to a presidential impeachment trial. From its first Whistleblower Protection Act in 1989 to Presidential Policy Directive 19 (PPD19), which protects federal employees of the Intelligence Community, the United States has aimed to extend protections to whistleblowers reporting waste, fraud, and abuse. Through OGP action plans, the United States has committed to advocating for legislation, exploring executive authority, and expanding and strengthening whistleblower protection. Most importantly PPD19 extended the rights of whistleblower protection to *private sector contractors* involved in national security operations. This has been an essential reform as it creates a formal channel for private actors to notify Congress and others of waste, fraud, and abuse. Such a channel did not exist at the time of the Snowden revelations in 2013.

## Private sector transparency regulation

- **Prior and informed consent in terms of service** - Establish a requirement of free, prior, informed consent for data processing. This should, at a minimum, require opt-out options for digital services and the ability to restrict data transfers.
- **Fiduciary risk disclosure**
  - For publicly traded companies listed on official stock exchanges and public employee pension plans, require quarterly *public* disclosure to regulators and shareholders on major actions impacting privacy or creating a *risk* of liability for privacy.
  - Require major lending institutions require disclosure of privacy impact and risk in annual reports.
- **Telecommunications and ISP transparency reporting -** Require or coordinate private companies and telecommunications utilities to publish official government requests for content removal, warrants, unwarranted requests for content removal, and other cooperation through transparency reports. Example.
- **Procurement blacklist -** Establish and maintain a publicly searchable blacklist/database of private sector contractors who have been found by oversight authorities to have violated the right to privacy. Ensure that all beneficial owners (above 10%) are included in the blacklist and that such data is required to be regularly updated and interoperable with company and ownership registries, politically exposed persons databases, and official asset disclosure databases.

### South Africa and Brazil: Emerging Data Protection Authorities

Middle income countries are increasingly interested in becoming part of the "fourth industrial revolution," powered by big data and analytics. They are seeking to import and export digital goods and services, and equally important to ensure that citizens are safe and able to adapt to an economy based on science, technology, and innovation. As part of this, both countries have introduced strong data protection authorities.

South Africa's "Information Regulator" is able to carry out independently initiated investigations and receive public complaints. In addition, it can train authorities and private actors on how to become compliant. As a major exporter of goods and services to the rest of the continent, because of its regulatory capacity, South Africa will be able to act as a bridge between markets in Africa and other regions. Notably, South Africa's information regulator is the same body that works on data protection.

Brazil's information regulator the National Authority for Data Protection (Autoridade Nacional de Proteção de Dados or "ANPD") was established by executive order in 2018. The 2020 data protection law enshrines this de facto independent body. It is able receive public complaints and to publish studies or release metadata on the state of privacy protection. One criticism has been that the agency does not have adequate independence from the office of the president.

## Records management

- Establishment of **limitations of the right to privacy** for holders of public office and government employees in their duties as public officers. This would minimize the ability to use take down requests on public records or protected speech. (The Grand Chambers of the European Union, for example, have ruled this illegal. The European Court of Human Rights has significant case law on balancing the right to information and personal data protection.)
- **Historical archives declassification -** In cases of national security or privileged information, require declassification of security documents after a set time period. Establish declassification as automatic and default, requiring agencies to request continued classification. After continuous civil society criticism, the US made a significant number of steps on security declassification through OGP, including unexpectedly declassifying its drone program in 2016.
- **Publishing metadata on classified documents.** By publishing metadata on classified records (with appropriate removal of high-risk information), future researchers will be able to corroborate metadata with actually released information. (See Canada "Records management" below.)
- **Records disposal -** Establish processes for systematic disposal of private personal data after a certain time period. Where there are pending legal cases, establish procedures for maintaining those records.

### Canada: Records management for right to information

Across its different OGP action plans, Canada has implemented commitments to open its records and improve its archives to enable for future retrieval of government-held information. Canada has taken steps to ensure that record management enables better access including:

- Granting public access to government archives and libraries,
- Making classified information available online,
- Revising regulations on document classification, and
- Establishing a unified recordkeeping system across agencies and levels of government.