ENHANCING DIGITAL CIVIC SPACE THROUGH THE OGP PROCESS

Principles and Recommendations for Enabling Reforms

ICNL
INTERNATIONAL CENTER
FOR NOT-FOR-PROFIT LAW

ENHANCING DIGITAL CIVIC SPACE THROUGH THE OGP PROCESS

Principles and Recommendations for Enabling Reforms

ICNL
INTERNATIONAL CENTER FOR NOT-FOR-PROFIT LAW

Published in August 2023

ACKNOWLEDGEMENTS

ICNL gratefully acknowledges the inputs into this resource of the following colleagues and partners: Digital Agenda for Tanzania Initiative (DA4TI); Francesca Fanucci and Karolina Iwanska, European Center for Not-for-Profit Law (ECNL); Natalia Carfi, Open Data Charter; Tonu Basu and Joe Foti, OGP Support Unit; and Orkidea Xhaferaj, Science & Innovation for Development (SciDEV).

ABOUT ICNL

The International Center for Not-for-Profit Law (ICNL) works with governments, civil society organizations, and the international community in more than 100 countries to improve the legal environment for civic space around the world. We believe that when people have the space to come together, positive, lasting change can be made. To achieve this vision, individuals must be able to join together, speak out, and take action to make the world a better place. Since 1992, ICNL has worked with our partners at all levels to promote and protect an enabling legal environment for civil society. Our international staff includes experts in all aspects of the laws governing free association, assembly, and expression, spanning from the local to global contexts. We also foster a worldwide network of organizations and individuals with in-depth expertise on a diverse range of issues relevant to civil society.

ICNL's programs include a range of initiatives specifically focused on promoting digital civic freedoms. ICNL works closely with our global network of partners to develop norms and standards so that new technologies protect basic freedoms and build an enabling environment for civil society. We also aim to enhance the fluency of civil society actors in technology so that they can participate meaningfully in crafting policies that affect civic space, and conduct research to collect best practices and identify challenges related to technology and civic space.

Learn more about our work at: www.icnl.org/our-work/technology-civic-space.

GREATER INTERNET FREEDOM

Internews

ICNL INTERNATIONAL CENTER FOR NOT-FOR-PROFIT LAW

The International Center for Not-for-Profit Law drafted this resource through support from the Greater Internet Freedom project, an initiative led by Internews and funded by USAID.

TABLE OF CONTENTS

Foreword

The core of open government lies in empowering citizens to contribute to accountable, responsive, democratic governance. As OGP co-chairs, we have seen the promise of digital technologies to bring government closer to the people, and to energize communities and civil society to make government more efficient, effective, and inclusive. From e-participation platforms, to digital service delivery portals, to online repositories of information about government programs, projects, and spending, digital technologies are an essential instrument in the open government reformer's toolkit. It is our faith in the democratizing potential of these technologies that has led Estonia, for instance, to commit through the OGP process to developing a new information system for involving citizens in policy development, and to deliver on this commitment with the Rahvaalgatus.ee platform, through which users can submit, support, and track citizen-sourced initiatives within the Parliament.

At the same time, we know digital technologies are not a panacea for open government. Platforms cannot substitute for genuine commitment to citizen engagement and empowerment. By itself, no digital portal or app can make policy more transparent, co-creative, or accountable if there isn't a culture of transparency and dialogue within government, and an environment that allows the public to exercise their voice. And as our lives move online, and governments increasingly employ digital tools to advance programs and policies, it becomes ever more important to co-create frameworks with diverse stakeholders that can govern the use of these tools to promote transparency, inclusion, and respect for human rights. It is in recognition of this reality that the new OGP Strategy calls for the development and use of digital technologies to be complemented by action to advance "democratization and governance of digital tools" and "measures and tools to promote democracy." The Strategy also prioritizes action across the Partnership to "protect and expand space for civil society and democratic dialogue."

We welcome this resource – developed by ICNL in cooperation with OGP and local and international partners – which sets forth

> By itself, no digital portal or app can make policy more transparent, co-creative, or accountable if there isn't a culture of transparency and dialogue within government, and an environment that allows the public to exercise their voice.

principles, recommendations, and positive examples of reforms to enhance digital civic space. We encourage the OGP community to build on this resource, through further exchange, innovation, and co-creation, to create more space for the exercise of digital freedoms. And we underline the crucial role of civil society in representing communities, highlighting challenges, and co-creating these reforms. We hope that civil society and government reformers alike will be able to use this resource, including through the Partnership-Wide Challenge launched at the 2023 OGP Global Summit in Tallinn, to advance the open digital space that is needed to promote real participation, transparency, and accountability – and to realize the promise of digital technologies for open government.

Taimar Peterkop
SECRETARY OF STATE
GOVERNMENT OF ESTONIA

Anabel Cruz
DIRECTOR
ICD URUGUAY

2022-2023 OGP Co-Chairs

1. Introduction

Digital technologies can make a substantial contribution to advancing open government. As many OGP governments have shown, digital tools can help agencies and officials share information and data with citizens, thereby improving access to services, advancing accountability, and countering waste and corruption.

But fostering digital open government requires more than just promoting information sharing through digital platforms. To truly empower citizens to participate in governance, OGP members need to preserve and promote digital civic space – the legal, social, and technological conditions that allow citizens to participate fully in the public sphere by exercising digital freedoms.[1] This requires investing in meaningful and inclusive access to digital services; protecting privacy rights online and offline; deploying rights-respecting approaches to address harmful information online; imposing appropriate safeguards on the use of artificial intelligence; and strengthening e-participation, open data frameworks, and civic engagement.

In this guide, we present recommendations for OGP commitments that can advance these aims, as well as examples of positive practices and policies that OGP members are already undertaking in these areas. We hope government representatives and civil society actors alike can draw on this resource to co-create enabling digital reforms.

But first, we begin by offering a checklist of principles to consult prior to embarking on digital policy initiatives, to ensure these actions respect and promote digital civic space.

2. Digital Civic Space Checklist

When governments design and implement digital policies, frameworks, and tools, they can do so in ways that foster inclusion, participation, and respect for human rights – or in ways that have unintended negative impacts or fail to achieve meaningful impact on open government. The following checklist offers guiding principles and relevant questions that should be considered prior to advancing a new policy or commitment related to technology:

- **Does the proposed digital initiative complement existing efforts to advance open government?** Digitization is not a substitute for focused efforts to enhance participation, transparency, access to information, and inclusion. What are your country's current commitments in these areas, and how does digitization support those efforts?

1 We use the term "digital freedoms" to encompass the set of civic freedoms – including rights to freedom of association, peaceful assembly, expression, participation, and privacy – that individuals exercise through use of digital technology, including online, or whose exercise may be significantly impacted by laws and policies governing the use of digital technology, including surveillance technology.

- **Is any proposed digital initiative designed to respect human rights and advance principles of good governance?** Do digital reforms first undergo a human rights risk assessment and are the principles of fairness, transparency, and accountability factored into their design? Transparency includes making available the purpose, processes, and outputs of tech systems in a way that is understandable and accessible to the public.

- **Does the proposed initiative work for the people, and not just for the government?** Were impacted communities consulted? Does the system only enable the government to share information, or does it also enable meaningful participation and two-way communication, such as feedback, complaints, or dialogue from the public?

- **Do digital solutions and legal approaches address a real need without introducing additional complications?** Governments should avoid assuming that more complicated or elaborate digital initiatives are necessarily better: launching a new portal when an email address would be sufficient, for instance, or passing a "fake news" law when civil defamation laws are adequate. Also, how does the solution or law impact women, girls, LGBTQ+, racial and ethnic minorities, and other marginalized groups who experience disproportionate harms online and barriers to internet access?

- **Do investments in digitization prioritize digital skills development, digital and media literacy, and meaningful, inclusive access?** Does the government have a plan to bridge digital divides to avoid excluding marginalized communities or exacerbating existing inequalities? Are there programs that empower citizens, public officials, and CSOs to effectively engage in digital governance processes? Have platforms been designed for language inclusivity (including minority languages) and for accessibility to those with sight and learning impairments and those with limited literacy?

- **Have privacy and personal data protection been embedded in all digital laws, policies, and tools in order to build trust in the systems?** Has the government adopted regulatory safeguards and cybersecurity measures to prevent data breaches, unauthorized access, and compromises to individuals' personal information?

- **Do data protection laws avoid disproportionate restrictions on freedom of expression and access to information?** Does the data protection law or implementing regulations include sufficient guidance, drafted in consultation with human rights practitioners and other members of civil society, on how to balance competing rights?

- **Do digitization programs have a deliberate plan for data collection, analysis, and sharing?** Do the programs facilitate open data and access to information, and employ open standards to foster interoperability, responsible data sharing, innovation, and prevention of vendor lock-in? Have efforts to un-silo data across agencies been designed to avoid undermining individual due process and privacy rights?

- **Do proposals to use predictive AI and algorithmic decision-making adequately consider associated costs and human rights risks?** Do proposed systems have a core emphasis on fairness, accountability, and transparency? Do they ensure that tools perpetuating discriminatory biases are not deployed at any level of decision-making?

- **Have digitization frameworks been developed through inclusive processes?** These can include public consultations, expert roundtables, publication of negotiating texts, and reasonable deadlines for submission of comments from interested parties. Has the government engaged in multi-stakeholder processes for the design of both tech platforms and digital reforms, with an emphasis on innovative co-creation?

- **Has ongoing assessment and monitoring been built into digital reforms?** Will initiatives undergo the continuous iterative improvement needed to ensure relevance and effectiveness in addressing emerging challenges and technological advances?

- **Is there adequate investment in the resources and technical expertise needed for the effective oversight and enforcement of internet and data governance frameworks?** Do relevant actors within the public sector, as well as civil society, small businesses, and other low-resourced stakeholders have sufficient capacity and resources to enforce and comply with new laws? Do frameworks to promote open data, access to information, and e-participation include detailed training and implementation plans and redress mechanisms, to ensure follow-through?

3. Recommended Digital Civic Space Commitments

Intersection with OGP Challenge Areas

The commitments and recommendations listed below align with the OGP Partnership-Wide Challenge: an initiative to challenge all members of the Partnership to take up at least one thematic area encompassed within the challenge and show tangible progress over the next five years. Thus, members can advance their work on the following thematic areas by incorporating the suggestions described in this guide:

Digital Governance

Civic Space

Gender

Justice

Public Participation

Access to Information

A. MEANINGFUL INTERNET ACCESS

Access to the global internet is integral to individuals' and organizations' ability to exercise digital rights. While digital governance can improve transparency and access to information, increase the efficiency and quality of service delivery, and enable greater and more frequent communication between citizens and public officials, the lack of accessible and affordable internet exacerbates existing inequalities and exclusion of marginalized groups who do not have access to the internet and still solely rely on in-person and offline interactions. Other obstacles can hinder full access to the digital commons, too – from limited digital skills and literacy, to unnecessary conditions and taxes imposed on digital access, to blanket shutdowns of internet services. By increasing access and affordability for all people as a part of their digital governance agendas, and refraining from measures that constrain the exercise of freedoms online, governments can empower all citizens to take advantage of digital tools and to contribute, through digital pathways, to better and more accountable governance.

✔ Recommended Commitments

- Recognize internet access as a constitutional right and enabler of other fundamental rights, such as the rights to freedom of expression, peaceful assembly, and association.

- Prior to accelerating digitization efforts, prioritize investments in network infrastructure in underserved and unconnected urban and rural communities, setting up secure public WiFi access points, and incentivizing the development of community networks.[2]
- Implement policies that make the internet more affordable, not less. This may include instituting more consumer protections; rescinding existing taxes on broadband or cellular internet access; encouraging greater market competition; subsidizing the cost of connectivity for individuals with lower income and persons with disabilities; and prohibiting discriminatory consumer practices by internet service providers that disadvantage lower-income and marginalized communities.[3]
- Review official digital platforms and tools, including through public consultations, and make appropriate modifications to ensure accessibility and appropriateness for all sectors of society, including youth, women and girls, migrants and refugees, minority language speakers, persons with disabilities, and LGBTQ persons.
- Incorporate age-appropriate and accessible digital literacy education in all levels of primary and secondary school curriculum and provide opportunities for adult learners to gain the knowledge and skills needed to advance their digital literacy.
- Abandon SIM card registration requirements that create undue barriers to mobile connectivity. Forced registration excludes individuals who lack access to traditional or digital IDs, including for structural and socio-economic reasons, thereby infringing upon the right to freedom of expression, and may also constitute an overbroad and disproportionate interference with users' privacy rights.[4]
- Repeal the legal basis for any intentional disruption of internet access that renders the internet unusable in whole or in part, whether nationwide or in specific locations. This includes, but is not limited to, blanket internet shutdowns (e.g., internet kill switches), internet throttling, and blocking entire social media or messaging platforms.[5] States should conduct a thorough,

2 "Community networks deliver access to underserved areas with infrastructure built, managed and used by local communities, oftentimes in areas that are financially unattractive for mainstream internet service providers." World Wide Web Foundation, "Community networks: Internet for the people, by the people" (Sep. 2, 2019), https://webfoundation.org/2019/09/community-networks-internet-for-the-people-by-the-people-the-web-untangled/.

3 See Avani Singh, "Digital discrimination: The need to realise universal access to the internet" (Dec. 5, 2019), https://altadvisory.africa/2019/12/05/digital-discrimination-the-need-to-realize-universal-access-to-the-internet/.

4 Access Now, "Veto the SIM Card Registration Bill, Protect Fundamental Human Rights" (Feb. 18, 2022), https://www.accessnow.org/press-release/philippines-sim-card-registration-bill/.

5 UN Special Rapporteur on freedom of opinion and expression, et al.., Joint Declaration on Freedom of Expression and Responses to Conflict Situations (May 4, 2015), https://www.osce.org/files/f/documents/a/0/154846.pdf.

transparent review of the current legal and regulatory framework relating to the disruption of telecom services, including by inviting and incorporating feedback from all stakeholders, such as civil society, telecom and internet service providers, media, and the public at large.[6]

- Refrain from, and develop guidance and regulations for ministries and law enforcement officials clearly prohibiting, extralegal practices of shutting down, throttling, or blocking internet services, in whole or in part.
- Promote meaningful internet access through foreign policy by issuing guidance to embassies and working with likeminded governments to engage governments with practices of shutting down, throttling, or blocking internet services, in whole or in part. Ensure that coercive economic sanctions include exemptions for internet and tech services that enable the public, including journalists and human rights defenders, to meaningfully access and use the internet.
- Mandate public disclosure of agreements entered into by the government with telecommunication service providers that authorize the government to issue requests for data or order the restriction of access to services. Issue guidance and regulations prohibiting the inclusion in such agreements of terms preventing service providers from publicly reporting information and statistics on network disruptions and takedown orders.

Positive Examples

- **Colombia** created an interactive web platform and call center to promote access by blind and deaf citizens to public information and government services.[7]
- **Costa Rica**'s Supreme Court has declared that access to the internet is a fundamental right, similar to the rights to information and communication. Law No. 8660 of 2008 requires that telecommunication operators provide open access to network and services and non-discrimination between public and private users. Costa Rica also has an Internet Advisory Council that facilitates multistakeholder and interdisciplinary cooperation from government, academia, the private sector, and civil society in developing policy on internet governance and access.[8]
- **Lesotho** has a universal access fund that aims to provide affordable and accessible telecommunications services to all citizens, particularly those living in rural and underserved areas, by financing the expansion of mobile net-

6 Access Now, "#KeepItOn: frequently asked questions," https://www.accessnow.org/campaign/keepiton/keepiton-faq/.

7 Open Government Partnership: Colombia, "Access to Information for People with Disabilities (C00033)," https://www.opengovpartnership.org/members/colombia/commitments/CO0033/.

8 Organisation for Economic Co-operation and Development, Digital Economy Policy in Costa Rica, (Feb. 2020), https://www.oecd.org/costarica/digital-economy-policy-in-costa-rica.pdf.

works and the rollout of fiber-optic cables, which has in turn led to a significant increase in internet penetration rates.[9] Lesotho is turning now to invest in digital skills, including of women and girls.[10]

- **Tanzania** has established a Universal Communications Service Access Fund, which aims to support the provision of affordable and accessible communication services, including internet access, in underserved and rural areas.[11]
- **The United States** has allocated $65 billion to boost broadband deployment and adoption, with funds earmarked for broadband deployment in unserved and underserved communities, development of low-cost broadband options for eligible families, digital inclusion and digital equity programs, and investment in tribal and rural areas.[12]

B. PRIVACY RIGHTS AND SURVEILLANCE

For individuals to be fully empowered to engage online, their privacy rights must also be protected – so that all persons feel comfortable expressing themselves, accessing services, and coming together through digital platforms. This requires appropriate safeguards to protect personal data, including not only protecting collected data from breach and disclosure, but also ensuring that any collection and processing of personal information – including information about activists, human rights defenders, and journalists – is legitimate, transparent, and accountable. To promote the exercise of digital freedoms, moreover, both online and offline activity must be free from arbitrary or indiscriminate surveillance, and governments and companies should be barred from arbitrarily repurposing data collected for a defined purpose for other purposes. Only robust protections for privacy rights, both online and offline, can ensure safe spaces to exercise other digital freedoms.

✔ Recommended Commitments

Data Protection and Processing

- Implement comprehensive legal frameworks, applicable to both private and public sector entities, to protect personal data and create well-resourced and independent offices responsible for enforcement. Key elements of such frameworks include:

9 See Marcin Frąckiewicz, "Internet access in Lesotho" (May 22, 2023), https://ts2.space/en/internet-access-in-lesotho/; World Bank, Lesotho – Digital Economy Diagnostic (February 2020), https://documents.worldbank.org/en/publication/documents-reports/documentdetail/196401591179805910/lesotho-digital-economy-diagnostic.

10 Tsoinyana Rapapa, "Lesotho policy statement" (Sep. 26, 2022), https://pp22.itu.int/zh-hans/itu_policy_statements/tsoinyana-rapapa-lesotho/.

11 Beatrice Materu, "Bridging the digital divide to empower rural Tanzania" (June 15, 2023), https://www.thecitizen.co.tz/tanzania/news/national/bridging-the-digital-divide-to-empower-rural-tanzania-4270950.

12 Government Technology, "Breaking Down Broadband Funding in the Infrastructure Bill" (Nov. 8, 2021), https://www.govtech.com/network/breaking-down-broadband-funding-in-the-infrastructure-bill.

- Exceptions to data protection rules should be clearly defined and narrow. There should be no exemptions from the highest standards of data protection for public institutions, including law enforcement, national security authorities, and counterterrorism agencies.
- Data minimization requirements and purpose limitations should be enacted to ensure only data necessary for a specific purpose is processed and that data is not repurposed. All personal information must be secure and stored for a specified, limited time (no longer than necessary to fulfill the given purpose).
- Processing of data that reveals sensitive information, e.g., health, political views, sexual orientation, or ethnic background, should be allowed only in clearly defined situations.

- Enact laws and regulations giving individuals the right of access to their publicly or privately held data and information about its processing, rectification, and deletion, as well as rights of objection and access to legal recourse and redress mechanisms where data is used unlawfully. When personal data is used as part of automated systems, individuals should have the right not to be subject to automated decisions.
- Recognize certain communities and individuals, such as migrants, as "vulnerable data subjects." Apply greater oversight and higher protective standards to the processing of their personal data, including in the context of both government data collection practices and surveillance-based business models.[13]

State Surveillance Programs

- Impose limitations on the interception of communications (e.g., communication content, identity of the parties to the communications, location-track-

13 Access Now, "Joint statement: Mexico, Guatemala, Honduras, El Salvador and the United States must terminate their agreements on cross-border transfers of migrants' biometric data" (Mar. 23, 2023), https://www.accessnow.org/press-release/statement-terminate-agreements-biometric-data-migrants/.

Intersection of the Right to Privacy and the Right to Access Information

Data protection laws typically contain broad exceptions authorization the publication of personally identifiable information if it is provided by law or in the public interest. These provisions can be interpreted and applied arbitrarily to either violate privacy rights or disproportionately limit the public's access to information and data in the name of data protection. Therefore, governments should commit to providing detailed guidance on the impact of their country's data protection laws on their access to information and open data policies. This guidance should be developed in close consultation with civil society with sufficient time and opportunity for public input.

ing, IP addresses, the time and duration of communications, and communication equipment identifiers), consistent with principles of international law,[14] including, but not limited to:

- Requiring authorization by an independent and competent judicial authority of all surveillance actions, upon demonstration by law enforcement that there is a high degree of probability that a serious crime has been or will be carried out, and that such surveillance will lead to relevant and material evidence that will assist in preventing the alleged harm from taking place or prosecuting the perpetrator(s) of that harm. Where exceptions to application authorization requirements are afforded due to exigent circumstances, law enforcement should be required to seek independent judicial authorization after the fact.
- Limiting collection of evidence through surveillance to that within the scope and duration of an authorized investigation. Law enforcement should not retain excess information, and information collected through surveillance should only be used for the authorized purpose and duration, and be destroyed or returned after it has been used for that purpose.[15] These principles apply whether surveillance is traditional, digital, online, or offline, and whether the purpose is to investigate cybercrimes or ordinary crimes. Authorities should not apply different judicial and due process standards to cybercrime investigations.

- Curb mass surveillance practices whereby the government continually collects, analyzes, and retains information about large numbers of people without any suspicion that they are culpable of wrongdoing; such practices are incompatible with democratic governance and can be abused to target individuals during peaceful protests or other protected acts of speech and assembly. Thus, states should commit to:
  - Prohibiting the use of Remote Biometric Identification (RBI) and facial recognition technology in publicly accessible spaces. Surveillance drones should likewise be barred from deployment during protests;[16]
  - Banning law enforcement from accessing or purchasing geolocation and traffic data without a warrant.
  - Repealing any laws mandating the general or indiscriminate retention of

14 Necessary & Proportionate: On the Application of Human Rights to Communications Surveillance, "The Principles" (May 2014), https://necessaryandproportionate.org/principles/.

15 Id.

16 European Digital Rights, Prohibit all Remote Biometric Identification (RBI) in publicly accessible spaces (May 2022), https://edri.org/wp-content/uploads/2022/05/Prohibit-RBI-in-publicly-accessible-spaces-Civil-Society-Amendments-AI-Act-FINAL.pdf.

geolocation and traffic data held by private services;

- Banning the use of cell-site simulators without a warrant; and
- Prohibiting the deployment of technologies capable of mass surveillance or the retention of personally identifiable information in "smart city" projects.

- Subject private sector entities participating in the acquisition, generation, or processing of surveillance data through a government contract to appropriate safeguards, including prohibitions on using data collected for any other purpose; mandatory disclosure of data breaches and misuse; penalties for misuse of data; whistleblower protections; and reasonable data deletion schedules.[17]

Oversight of State Surveillance Programs

- To promote transparency with respect to state surveillance programs and technology:
  - Establish an independent oversight mechanism to ensure transparency and accountability of state surveillance programs. This mechanism should have the authority to access all potentially relevant information about State actions, including, where appropriate, access to secret or classified information, and to make referrals to a body with appropriate remedy and redress authorities;[18]
  - Require public disclosure of information about the procurement of new surveillance technology, including reporting on the technology's uses and impacts. This may include conducting and publicizing human rights impact assessments prior to the procurement of surveillance technology, as well as similarly publicized periodic audits.
  - Publish aggregate information on the specific number of requests for communication surveillance approved and rejected, with disaggregation of requests by service provider and by investigation authority, type, and purpose; and disclosure of the number of individuals affected by each type of request.[19]
  - Provide appropriate resources and ongoing training to anyone responsible for oversight, procurement, and impact assessments of surveillance technology, to ensure they are aware of the appropriate and lawful use of such technology, the technical limitations thereof, and data protection best practices.[20]

17 Freedom Online Coalition, Guiding Principles on Government Use of Surveillance Technologies (March 2023), https://freedomonlinecoalition.com/wp-content/uploads/2023/03/FOC_Guiding_Principles_on_Government_Use_of_Surveillance_Technologies.pdf.

18 Necessary & Proportionate, "The Principles," supra note 14.

19 Id.

20 Freedom Online Coalition, Guiding Principles, supra note 17.

Use and Trade in Surveillance Technologies

- At minimum, impose a moratorium on the use of facial recognition technology by government authorities, and as appropriate engage in fully inclusive and robust public consultation to design appropriate regimes for the regulation of this technology.
- At minimum, impose an immediate moratorium on the sale, export, import and deployment of spyware technologies until a robust regulatory framework is in place that includes prohibitions on the development, use, and export of invasive spyware. The export, import and deployment of spyware, such as Pegasus, fundamentally violates the right to privacy and, by silencing activists, journalists, and political opponents, can undermine the very essence of democracy and open government.

Positive Examples

- The government of **Catalonia** implemented a moratorium on the export, sale, transfer, and use of spyware technology until there are sufficient guarantees that this technology complies with human rights protections, thereby implementing the Geneva Declaration on Targeted Surveillance and Human Rights.[21]
- **Brazil** has passed a General Law on Protection of Personal Data, which requires consent for processing of biometric data except under certain circumstances, and which guarantees the right of the data subject to request review of decisions made solely based on automated processing of personal data and affecting his/her interests.[22]
- Under **Estonia**'s amended 2018 Personal Data Protection Act, and consistent with the EU General Data Protection Regulation (GDPR) and Law Enforcement Directive, any official processing a citizen's data for a purpose other than a criminal investigation must inform the citizen of the purpose, as well as the official's name and contact information.[23]
- **Georgia** committed to publishing statistics on requests for covert investigative actions (i.e., surveillance) submitted by law enforcement agencies to the courts.[24]
- **Morocco** instituted a temporary moratorium on the use of facial recognition technology from September 2019 to the end of 2020, to provide an op-

21 Catalan News, "Catalonia first after US to restrict Pegasus spyware use" (Apr. 4, 2023), https://www.catalannews.com/politics/item/catalonia-first-after-us-to-restrict-pegasus-spyware-use.

22 Brazilian General Data Protection Law (2019), available in English translation at https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/.

23 Personal Data Protection Act (2018), available in English translation at https://resources.law.cam.ac.uk/cipil/documents/GDPR_English_From_Official_Bodies/Estonia%20-%20GDPR%20Implementation%20Act.pdf.

24 Open Government Partnership: Georgia, "Proactive Publishing of Surveillance Data (GE0027)," https://www.opengovpartnership.org/members/georgia/commitments/GE0027/.

portunity for broad consultation of both public and private actors, including civil society, on how to proceed with regulation of facial recognition.[25]

- The **United States** has barred operational use of foreign or domestic commercial spyware by all U.S. federal agencies, unless they meet stringent requirements.[26]
- Cities in the **United States**, including Minneapolis,[27] Boston (with carve-out for facial recognition evidence collected by other agencies or groups),[28] and Oakland,[29] have passed ordinances banning acquisition or use of facial recognition technology. The U.S. state of California has passed a law prohibiting the use of facial recognition and other biometric surveillance with police body cameras.[30] And the U.S. state of Illinois has passed a law requiring private entities in possession of biometric identifiers and information to develop a publicly available retention schedule and guidelines for destruction of collected identifiers and information; and to store, transmit, and protect from harm these identifiers and information using the reasonable standard of care in the industry. BIPA also prohibits private entities from obtaining biometric identifiers or information without providing written notification to the subject; from profiting off people's biometric information; and from disseminating biometric information without first obtaining consent of the subject. BIPA creates a cause of action and has been construed to have broad standing requirements.[31]

25 Biometric Update, "Morocco extends facial recognition moratorium to year-end, proposes biometric authentication service" (Apr. 9, 2020), https://www.biometricupdate.com/202004/morocco-extends-facial-recognition-moratorium-to-year-end-proposes-biometric-authentication-service. Since 2021, however, the government of Morocco has moved forward with facial recognition programs in the Rabat airport and as part of the smart city initiative in Casablanca, and it is unclear what safeguards and privacy protections will be enforced as part of these initiatives. See, e.g., Dima Samaro, "Pandemic tech and digital rights in Morocco" (Mar. 30, 2022), https://globalvoices.org/2022/03/30/pandemic-tech-and-digital-rights-in-morocco/; Lamine Rahhali, "ONDA Opens Tender for New Face ID Recognition System in Rabat Airport" (Aug. 4, 2022), https://www.moroccoworldnews.com/2022/08/350633/onda-opens-tender-for-new-face-id-recognition-system-in-rabat-airport.

26 Access Now, "No to spyware: Biden administration bars U.S. federal government from using rights-abusing tech" (Mar. 23, 2023), https://www.accessnow.org/press-release/no-to-spyware-us/.

27 Ordinance Amending Title 2, Chapter 41 of the Minneapolis Code of Ordinances relating to Administration: Information Governance (2021), available at https://lims.minneapolismn.gov/Download/File/4860/Facial%20Recognition%20Ordinance%2001.21.2021.pdf.

28 Ordinance banning facial recognition technology in Boston (2020), available at https://www.documentcloud.org/documents/6956465-Boston-City-Council-face-surveillance-ban.html.

29 Regulations on City of Oakland's Acquisition and Use of Surveillance Technology, available at https://library.municode.com/ca/oakland/codes/code_of_ordinances?nodeId=TIT9PUPEMOWE_CH9.64REACUSSUTE.

30 An act to add and repeal Section 832.19 of the Penal Code, relating to law enforcement (2019), available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1215.

31 Biometric Information Privacy Act (2008), available at https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

ISSUE IN FOCUS

Digital ID

Governments that adopt digital ID frameworks bear a particularly high responsibility to ensure the protection of personal data prior to adopting such frameworks. Digital ID poses many threats to democratic governance, allowing for concentration of information, increased control, and increased risks of surveillance of citizens. Furthermore, in countries where digital skills are still at low levels, digital ID systems can increase the risk of exclusion, especially of marginalized and vulnerable groups. In most contexts, the security risks related to a centralized system of highly sensitive and personal data currently outweigh the benefits.

Principles to keep in mind in designing digital ID systems include:

- **Privacy-Enhancing Design**: Ensure that digital ID systems are designed with privacy as a core principle, and that these systems incorporate privacy-enhancing technologies and techniques such as decentralized identity, zero-knowledge proofs, and strong encryption to protect individuals' personal information.
- **Consent and Control**: Establish mechanisms to obtain informed consent from individuals for the collection, use, and sharing of their identity data, and provide individuals with granular control over the disclosure and use of their digital ID information.
- **Interoperability and Portability**: Promote interoperability and portability of digital ID systems, allowing individuals to use their digital ID across different services, platforms, and sectors, while ensuring data protection and privacy standards are maintained.
- **Security and Fraud Prevention**: Implement robust security measures to protect digital ID systems against unauthorized access, identity theft, and fraud, such as multi-factor authentication, secure storage, and identity verification processes.

In implementing digital ID programs, governments should:

- Conduct a robust human rights and privacy impact assessment prior to designing or adopting a digital ID framework, that includes risk mitigation measures to ensure that the data of citizens and residents are protected. The assessment should be transparently shared and open to feedback from the public.
- Implement digital ID as a voluntary government service through which citizens and residents can enroll if they prefer to manage their government interactions digitally. Continue to allow individuals to prove their identity using conventional identification.
- Refrain from collecting and integrating biometric data as part of a digital ID system until the government can guarantee the data can be collected accurately and securely and the data can be stored without the risk of unauthorized access.
- Do not establish digital ID systems as a centralized repository that government officials can easily access without limitations, particularly if the digital ID system includes biometric data. Access to the data should be strictly limited, and law enforcement access should be predicated on a warrant issued by an independent judicial authority.

C. ARTIFICIAL INTELLIGENCE

The use of AI must benefit individuals and society. Yet, the development and deployment of AI systems have far outpaced regulation and oversight. To ensure that the benefits of such systems outweigh the risks to human rights,[32] and that adequate accountability mechanisms are in place to address harms when they occur, it is essential to put in place systematic means for transparency, oversight, and redress – especially when States adopt AI in the context of democratic processes, service delivery, and criminal justice mechanisms. Governance of AI systems should follow a human rights-based approach, guided by international human rights law and standards and relevant jurisprudence, rather than an ethics-based approach.[33] And governance frameworks should not include exemptions for AI systems deployed for purposes of law enforcement, migration, justice, national security, and counterterrorism; rather, it is particularly important to ensure the fairness, transparency, and accountability of such systems, given the severe impacts on human rights that may result from their deployment.

✔ Recommended Commitments

- Undertake human rights impact assessments when designing, developing, procuring, or deploying AI systems, especially in the context of democratic processes, law enforcement activities, judicial proceedings, and social safety net services. Human rights impact assessments of AI systems should include consultation with civil society actors and other experts and be validated by an accredited external independent oversight body with human rights expertise. Results of such assessments should be made public.

Governance frameworks should not include exemptions for AI systems deployed for purposes of law enforcement, migration, justice, national security, and counterterrorism; rather, it is particularly important to ensure the fairness, transparency, and accountability of such systems, given the severe impacts on human rights that may result from their deployment.

32 Risks to human rights posed by AI include, but are not limited to: discrimination as a result of biased training or input data; restrictions to the right to freedom of expression resulting from use of AI for content moderation; disproportionate infringement of the right to privacy due to mass data collection and surveillance (including during protests); and violation of the right to effective remedy when the complexity and opacity of an AI system obscures accountability for harms caused by the system.

33 Ethics is a branch of philosophy that lacks normative consensus. Human rights, in contrast, "is a crystallization of ethical principles into norms, their meanings and implications well-developed over the last 70 years. These norms command high international consensus, are relatively clear, and can be developed to account for new situations. They offer a well-calibrated method of balancing the rights of the individual against competing rights and interests using tests of necessity and proportionality." Kate Jones, AI governance and human rights: Resetting the relationship (2023), https://www.chathamhouse.org/sites/default/files/2023-01/2023-01-10-AI-governance-human-rights-jones.pdf.

- Develop guidance, through inclusive and robust public consultations including civil society, experts, and representatives of relevant communities, to guide government agencies in determining whether to deploy algorithmic decision-making systems.
- Enact policies that ensure people affected by AI systems are aware when AI systems are deployed, as well as their impacts. If an AI system causes harm, the affected individual should have access to effective redress options.
- Publish information about the use of algorithms in public decision-making, including the purpose of the algorithm; optimization goals; how and on what data the algorithm was trained; its input and output data, parameters, loss functions, and underlying assumptions; and when practicable, the source code.
- Ban the use of AI systems that pose unacceptable risks to human rights. These include predictive AI systems for policing and profiling, predictive systems used to curtail and prevent migration, predictive systems for assessing personality used in judicial proceedings, and remote biometric identification in publicly accessible areas.
- Review regulatory frameworks on AI, with appropriate and inclusive public consultation, and remove blanket national security or counterterrorism exemptions from requirements governing the transparency, accountability, accuracy, and quality of AI systems.

Positive Examples

- **Brazil** created an independent commission made up of legal experts to study the risks and impacts of AI as well as the different approaches to addressing AI through regulation. In addition to its own research, the commission convened multistakeholder public briefings to gather insights from civil society, academics, the private sector, and regulators in other jurisdictions, and then issued a report presenting recommendations for draft legislation to the Federal Senate.[34]
- **Canada** has issued a directive mandating algorithmic impact assessments before production of any automated decision system; provision of advance notice that decisions will be rendered in whole or in part by automated decision systems; development of systems to test ADS for bias, inaccuracy, and compliance with privacy requirements; and release of relevant source code.[35] **Canada** has also committed to improving transparency and awareness of the Government's use of artificial intelligence, including by developing a

34 Cristina Akemi Shimoda Uechi & Thiago Guimarães Moraes, "Brazil's path to responsible AI" (July 27, 2023), https://oecd.ai/en/wonk/brazils-path-to-responsible-ai.

35 Government of Canada, Directive on Automated Decision-Making (2019), https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592.

Treasury Board directive on decision support systems to set rules on how departments can use AI ethically to make decisions, as well as an algorithmic impact assessment tool to help institutions better understand and mitigate the risks associated with automated decision-making systems.[36]

- The **European Union** is currently drafting the first law on AI to be put in place by a major regulator, which assigns applications of AI to four risk categories. First, applications and systems that present a clear threat to the safety, livelihoods and rights of people – such as government-run social scoring programs – will be deemed to pose an unacceptable risk and will be banned. Second, high-risk applications, including all remote biometric identification systems, will be subject to strict legal requirements before they can be deployed. Third, AI systems presenting "limited risks," including chatbots, will be permitted with specific transparency obligations. Lastly, AI systems considered to present minimal risk will be freely permitted and largely left unregulated.[37]

- In the **European Union**, the GDPR guarantees the right for an individual not to be subject to decisions based solely on automated processing that produce legal or other significant effects on that individual; requires entities using automated decision-making to implement measures to protect the rights, freedoms, and legitimate interests of affected persons, including the right of such persons to obtain human intervention and to contest the decision; and guarantees the right to know of the existence of automated decision-making. The GDPR also requires that a data protection impact assessment be conducted when a type of processing using new technologies is likely to result in significant risks to the rights and freedoms of natural persons, such as when automated processing is used for systematic and extensive evaluation of personal aspects that produce legal or other effects on natural persons.[38]

- **France** has prohibited the use in court decisions of automated assessments of a person's behavior (i.e., automated decision-making "intended to assess certain aspects of that person's personality").[39] **France** has further committed to publishing public algorithms to improve the transparency of source codes and is working within its government to develop a shared methodolo-

36 Open Government Partnership: Canada, "Digital Government and Services (CA0067)," https://www.opengovpartnership.org/members/canada/commitments/CA0067/.

37 European Commission, "Regulatory framework proposal on artificial intelligence," https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai. In the position adopted by the European Parliament on the AI Act, it has pushed for even broader protections, including the full prohibition of the development and use of remote biometric identification (RBI), e.g. facial recognition, in real time. See European Center for Not-for-Profit Law, "Big Win for Fundamental Rights, As the European Parliament Adopts the AI Act" (June 14, 2023), https://ecnl.org/news/big-win-fundamental-rights-european-parliament-adopts-ai-act.

38 EU General Data Protection Regulation, available at https://gdpr-info.eu/.

39 LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037085952/.

gy for more open information systems.[40]

- The **Netherlands** drafted and mapped frameworks and guidelines as a tool for government organizations to use in determining whether to make algorithms openly available,[41] and has committed to conducting fundamental rights impact assessments of all algorithms deployed for public sector uses.[42]
- **New Zealand** conducted a review of existing operational algorithms and their use across a range of government agencies, and developed a draft Algorithms Charter that sets standards for safe and ethical use of algorithms by public-sector agencies and guidance for meeting transparency and accountability objectives.[43]

D. ADDRESSING HARMFUL INFORMATION ONLINE

Disinformation, tech-facilitated gender-based violence (TFGBV), and hate speech greatly impact online civic space and democratic processes. Disinformation increases polarization, has the potential to influence elections, and can fuel violence. Meanwhile, TFGBV and hate speech discourage and prevent women, girls, ethnic and religious minorities, and other individuals from marginalized communities from actively participating online. While the harms are real, accurate identification of disinformation, hate speech or misleading content is extremely difficult and context-sensitive. Some government responses to these harms have disproportionately curtailed the freedom of expression. Governments should take steps to promote healthy and safe information ecosystems online while also protecting the exercise of online civic freedoms.

✔ Recommended Commitments

- Revise relevant laws to authorize the investigation and prosecution of cyberstalking, online sexual harassment, online posts of non-consensual sexual images, and other forms of tech-facilitated gender-based violence. Law enforcement should be equipped to investigate these incidents using trauma-informed practices.
- Enact measures to promote transparency about activities giving rise to disinformation, such as "anti-bot" laws requiring automated online accounts to reveal their identities to users under certain circumstances, or laws mandating

40 Open Government Partnership: France, "Transparency of Public Algorithms (FR0035)," https://www.opengovpartnership.org/members/france/commitments/FR0035/.

41 Open Government Partnership: Netherlands, "Open Algorithms (NL0031)," https://www.opengovpartnership.org/members/netherlands/commitments/NL0031/.

42 Government of the Netherlands, "Fundamental Rights and Algorithms Impact Assessment (FRAIA)," https://www.government.nl/documents/reports/2021/07/31/impact-assessment-fundamental-rights-and-algorithms.

43 Open Government Partnership: New Zealand, "Review of Government Use of Algorithms (NZ0019)," https://www.opengovpartnership.org/members/new-zealand/commitments/NZ0019/.

transparency about the origins of online advertising or sponsored content.[44]

- Invest in non-legal measures to counter harmful online content, such as media literacy programs, curriculum development for schools on how to critically assess information and news, and support to women and marginalized communities that are at greater risk of being targets for harmful content online.
- Publish regular reports with transparent information about all court-mandated content takedown orders and content takedown requests from other public authorities, including the number and type of requests, and their rationale.
- Convene diverse stakeholders – including digital platforms and other technology companies, civil society, academic experts, and representatives of communities frequently targeted by abusive online communications – to share information, identify research questions, and explore practices that can contribute to the development of healthy and safe online information ecosystems. Government should also encourage platforms and other technology companies to invest in capacity-building, reporting and dialogue mechanisms that can foster free exchange of information with civil society and the public, with the aim of promoting safe navigation of platforms and reducing the incidence of harmful information online.
- Repeal or amend existing laws to combat disinformation and other harmful information online if the laws do not precisely identify a specific harm[45] or are not narrowly tailored to address the harm. Vague and disproportionate laws that target online speech violate a State's human rights obligations and lead to censorship of otherwise protected speech. Engage in a multistakeholder, consultative process to ensure any legal

Countries should invest in non-legal measures to counter harmful online content, such as media literacy programs, curriculum development for schools on how to critically assess information and news, and support to women and marginalized communities that are at greater risk of being targets for harmful content online.

44 ICNL, Legal Responses to Disinformation (2021), https://www.icnl.org/wp-content/uploads/2021.03-Disinformation-Policy-Prospectus-final.pdf.

45 The harm must be to one of the following legitimate aims, as stipulated in international human rights law: national security, public order, public health, public morals, or the rights and reputation of others.

measures that restrict online speech are based on the State's human rights and constitutional obligations and high-quality research about the harm, its impacts, and its pervasiveness.

- Engage with human rights and child protection organizations as well as the public to review existing laws or bills related to protecting children online, to ensure that such laws are precise and narrowly tailored to protect children from online harms while avoiding infringement upon children's right to freedom of expression. Governments should further invest in non-legal measures that engage and educate children and parents about risks online and mitigation measures they can take.

Positive Examples

- The state of São Paulo in **Brazil** has offered media literacy as an elective class for middle schoolers. The class includes lessons on how to responsibly use the internet and recognize trustworthy information.[46]
- The Code of Practice on Disinformation was a voluntary initiative, undertaken based on guidance from the **European Commission**, under which 34 private-sector signatories committed to demonetizing the dissemination of disinformation; ensuring the transparency of political advertising; empowering users; enhancing the cooperation with fact-checkers; and providing researchers with better access to data.[47]
- **Finland** has developed a media literacy module that helps school-age individuals identify and distinguish amongst misinformation, disinformation, and mal-information.[48]
- **France** has committed to hosting multi-stakeholder dialogue with civil society and research institutions, to identify research priorities and existing tools, resources, and techniques to monitor and counter misinformation and disinformation, and to discuss proposed solutions to counter the dissemination of misinformation and disinformation.[49]
- The **Netherlands** has committed to introducing greater transparency into how political parties are funded while making online election campaigns and political

46 Estadão, Escolas da rede estadual de SP terão disciplina sobre fake news" (Nov. 21, 2019), https://www.estadao.com.br/educacao/escolas-da-rede-estadual-de-sp-terao-disciplina-sobre-fake-news/.

47 European Commission, "The 2022 Code of Practice on Disinformation," https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

48 Jon Henley, "How Finland starts its fight against fake news in primary schools" (Jan. 29, 2020), https://www.theguardian.com/world/2020/jan/28/fact-from-fiction-finlands-new-lessons-in-combating-fake-news.

49 Open Government Partnership: France, "Forum to discuss combatting disinformation (FR0106)," https://www.opengovpartnership.org/members/france/commitments/FR0106/.

advertisements more transparent, as a means of combatting disinformation.[50]

- In the **United States**, the state of California has enacted an "anti-bot law" that requires that bots (or the person controlling them) reveal their "artificial identity" when they are used to sell a product or influence a voter. The law defines a "bot" as "an automated online account where all or substantially all of the actions or posts of that account are not the result of a person."[51]
- In April 2019, six of **Uruguay**'s political parties signed an Ethical Pact Against Disinformation that pledged "not to generate or promote false news or disinformation campaigns to the detriment of political adversaries." The Uruguayan Press Association proposed the pact as one of three prongs to combat disinformation. The other two prongs were trainings for media professionals and fact-checking.[52]

ISSUE IN FOCUS

E-Participation and Civic Engagement

Government e-participation tools that use digital technologies to involve the public in policy-making, service design and delivery, and other decision-making have the potential to advance citizen engagement in open government. Such tools include online platforms designed to:

- share information about proposed law- and policy-making;
- provide opportunities for public feedback on proposed measures and the implementation of programs and policies;
- facilitate public identification of priority issues and the development of legal and policy proposals, including through e-petitions; and
- promote greater transparency and participation regarding public meetings and proceedings, through techniques such as live-streaming and remote participation.

In practice, however, investments in e-participation have often failed to achieve meaningful outcomes. To be impactful in advancing open government and digital freedoms, e-participation tools must go beyond simply creating e-portals and making information available online. Such programs must be part of a larger initiative to increase civic engagement and opportunities for two-way communication between public authorities and citizens, both online and offline – while promoting appropriate respect for the civic freedoms that undergird effective participation.

50 Kajsa Ollongren, "Transparency, Disinformation, and New Legislation for Political Parties" (May 29, 2019), https://www.opengovpartnership.org/stories/transparency-disinformation-and-new-legislation-for-political-parties/.

51 The National Law Review, "California's BOT Disclosure Law, SB 1001, Now In Effect" (July 15, 2019), https://www.natlawreview.com/article/california-s-bot-disclosure-law-sb-1001-now-effect.

52 APU.uy, "APU desarrolla seminarios en el interior contra las noticias falsas" (Dec. 6, 2019), https://www.apu.uy/noticias/apu-desarrolla-seminarios-en-el-interior-contra-las-noticias-falsas.

Principles to keep in mind when investing in e-participation tools include:

- **Privacy-Enhancing Design**: Ensure that e-participation tools include privacy as a core principle. The platforms should not require registration to contribute or collect unnecessary data about individuals or use cookies for unwanted tracking.
- **Holistic Approaches to Participation**: While social media engagement has many benefits and can reach different, diverse segments of the public, it has many limitations and should not form the sole basis of a public participation program. Governments should deploy trusted and secure online platforms to provide spaces for written or oral input, while maintaining and supporting traditional forms of engagement, such as community town halls and public hearings.
- **Creation of Feedback Loops**: Participation does not end when members of the public submit their input. The government must institute steps to evaluate and incorporate input into decision-making; provide information and data regarding comments received and how these have been addressed; and release revised policy documents for public review with sufficient time for additional consultation.
- **Continuing Investment**: E-participation tools and platforms do not, by themselves, yield public engagement and improved policymaking and program implementation. Generating these outcomes requires continual investment in publicizing tools and platforms; engaging in outreach to particularly affected communities; building the capacity of government officials to use new tools; and promoting institutional cultures that prioritize openness and value public input in decision-making.
- **Trusted Institutions**: If members of the public do not trust government institutions, they are unlikely to participate in government affairs, whether the opportunities are online or offline. Increasing trust in institutions is a long-term process that requires governments to respect and enforce their human rights obligations, increase transparency, reliably deliver services, and provide means for redress when individuals are harmed by government action or inaction. Technology that serves these purposes can accelerate trust-building; e-participation tools deployed without sufficient investment in trust-building, however, are unlikely to be effective.

In implementing e-participation tools to increase civic engagement, governments should:

- Embed e-participation programs in a larger effort to promote civic education in primary and secondary schools and advance inclusion of historically marginalized communities.
- Develop effective frameworks for e-participation that incorporate measures for meaningful participation at all stages of the decision-making process, including before, during, and after decision-making. To ensure meaningful participation, such frameworks should mandate sufficient advance notice of participation opportunities; publication of relevant materials in advance; provision of adequate time to provide inputs; feedback on how inputs have been addressed (see also below); and remedies where prescribed participation processes have not been followed.
- Undertake a comprehensive study of the use of current e-participation tools, gaps in the use and efficacy of such tools, and the resources and capacities needed to set up inclusive and meaningful e-participation platforms. The study should engage and collect input

from public servants, technologists, civil society, members of the public, and the business community. The study can be shared with the public and be used to inform national plans for designing, adapting, and deploying e-participation tools.

- Design (or adapt) and deploy e-participation tools in ways that are inclusive and participatory, using methods of co-creation to ensure the tools address needs and challenges surrounding public engagement based on the local context.
- Ensure open and transparent procurement of e-participation tools and platforms.
- Design and test accessibility features for persons with disabilities prior to releasing new e-participation tools or platforms.
- Recognize that a robust, pluralistic, and independent civil society is a prerequisite to successful e-participation initiatives. Civil society can create bridges between governments and constituents, consolidate and contextualize inputs, and leverage trust developed in communities to reach individuals who otherwise would not engage with government platforms. To empower civil society to play this role, governments must reduce and remove restrictions on the ability to form associations, peacefully assemble, engage in online or offline expression, and access domestic or foreign funding.

E. OPEN DATA AND ACCESS TO INFORMATION

The right to access information and open government are interconnected, and free access to government data is a key component of the right to access information. Through expanded access to aggregated data and government documents related to decision-making, policy, and service delivery, civil society and citizens can better monitor whether governments are fulfilling their obligations and commitments. Researchers can also use publicly available data to help the government identify gaps and areas where policy or service delivery could be improved. Some data, such as personally identifiable information or data about military operations, might be highly sensitive and warrant protection from disclosure. But for the majority of government data, free and open access can provide a basis for public engagement on the design, implementation, and monitoring of policies and programs, including on many of the topics addressed elsewhere in this guide – from prevention of disruptions to internet service, to imposition of appropriate limitations on government surveillance, to furthering governance and oversight of algorithmic decision-making, to adoption of appropriate measures to address harmful information online.

✔ Recommended Commitments

- Appoint responsible public officials (open data "champions") in each relevant agency and office to implement the plan and ensure they are properly trained on the data collection principles, methods, and tools. Training should be ongoing.

- Include easy-to-understand explanations of the datasets, publishing videos in local languages to explain how the public can make use of the data, and/or holding virtual or in-person open data events. Videos and explanations could include case studies of how the data was effectively used.
- Create mechanisms by which the public can provide feedback on the datasets, such as through rating systems or discussion forums. Engage the public in participatory processes to create publication plans for datasets, to connect data demand with actual governmental capacities and manage expectations on both sides.
- Monitor open data implementation and public use of the data to adapt and improve upon the type of data that is shared, the processes for collection and publishing of data, and the systems and tools that are used. Use lessons from this monitoring to inform the design or modernization of data systems, so that public officials in charge of open data can more readily draw on these systems to prepare datasets for publication.

Positive Examples

- As part of its 2017-2019 Action Plan, **Argentina** created a public database of audit recommendations and compliance information from the Federal Prison Service. Government collaborated with academia and civil society to ensure the final design significantly increased CSOs' ability to monitor the penitentiary system. The government's 2019-2021 Action Plan aimed to further strengthen public oversight of the prison system by establishing a National Penitentiary Diagnosis, an annual study that will be collaboratively designed by the government, CSOs, and academia to evaluate the penitentiary system from a human rights perspective.[53]

> **For the majority of government data, free and open access can provide a basis for public engagement on the design, implementation, and monitoring of policies and programs, including on many of the topics addressed elsewhere in this guide.**

53 OGP, "Open Prison Data and Civil Society Oversight in Argentina" (Mar. 23, 2021), https://www.opengovpartnership.org/stories/open-prison-data-and-civil-society-oversight-in-argentina.

- **France** implemented new open data clauses in government contracts to increase competition between firms applying for these contracts and promote better services.[54]
- In **Korea**, the government has announced a National Core Data Release Plan to help identify and release economic data that citizens want. To identify and select data to be released as National Core Data, the government obtains feedback from the Open Data Forum and performs demand surveys of citizens and businesses. National Core Data projects are then selected by the Open Data Strategy Council, a multi-stakeholder body established under the prime minister to monitor the government's major open government data policies, plans, and implementation.[55]
- **Moldova**'s e-procurement system MTender, launched as a pilot in 2017, made readily available significant information on procurement procedures, enabling every interested citizen to find relevant data on a certain public authority and the procedures it conducts. The Moldovan CSO Association for Efficient and Responsible Governance (AGER) has complemented these disclosures by empowering civil society to track and report irregularities, including through a new page on the platform that focuses on explaining the most frequent irregularities and supporting civil society in using open data for increasing the accountability of public authorities.[56]

54 OGP, "Open Data Laws in France Increase Competition for Public Contracts" (Sep. 20, 2021), https://www.ogpstories.org/open-data-laws-in-france-increase-competition-for-public-contracts/.

55 Hyejeong Lim, "Open Data to Improve Transparency and Drive Growth" (Mar. 13, 2023), https://www.ogpstories.org/open-data-to-improve-transparency-and-drive-growth/.

56 Maria Covalciuc, "Detecting Budget Fraud Through Citizen Monitors" (Apr. 14, 2022), https://www.ogpstories.org/detecting-budget-fraud-through-citizen-monitors/.


ICNL
INTERNATIONAL CENTER
FOR NOT-FOR-PROFIT LAW
Open
Government
Partnership