46th Closed Session of the Global Privacy Assembly (GPA)
October 2024

Resolution on surveillance technologies and protecting individuals' rights to privacy

This Resolution is submitted by:

SPONSORS *:*

- CNDP Morocco (National Commission of the control of Personal Data protection)
- INAI Mexico (National Institute for Transparency, Access to Information and Personal Data Protection)
- AAIP Argentina (Agency of Access to Public Information)

CO-SPONSORS *:*

- CIL Burkina Faso (Commission de l'Informatique et des Libertés)
- Office of the Data Protection Authority of Guernsey

The 46th Annual Closed Session of the Global Privacy Assembly (GPA) 2024:

Recognizing the establishment of a sub-group on surveillance technologies within the DESWG *(Digital Economy and Society Working Group)* of the Global Privacy Assembly (GPA) and their efforts to deliver relevant insights on this subject by conducting research, carrying out a literature review, and developing topical papers;

Considering the ongoing global debate on the development of surveillance technologies among a diverse set of stakeholders (including regulators, lawmakers, developers, users, academia, researchers and civil society), and their respective perspectives on the opportunities and risks of surveillance technologies, set out in investigative findings, white papers, scientific papers, articles and other public communications;

Recalling the GPA past-resolutions, in particular on Privacy by Design (2010)[1], on Big Data (2014)[2], Conference Communiqué on AI and surveillance/law enforcement access to data (2016)[3], on ethics and data protection in artificial intelligence (2018)[4], on government access to data, privacy and the rule of law: principles for government access to personal data held by the private sector for national security and public safety purposes (2021)[5] and GPA

[1] Resolution on Privacy by Design (globalprivacyassembly.org)
[2] Resolution A - Big Data EN (globalprivacyassembly.org)
[3] https://globalprivacyassembly.org/wp-content/uploads/2015/02/ICDPPC-Newsletter-Volume-3-edition-1-November-2016-.pdf
[4] 40th International Conference of Data Protection and Privacy Commissioners, Brussels (globalprivacyassembly.org)
[5] 20211025-GPA-Resolution-Government-Access-Final-Adopted .pdf (globalprivacyassembly.org)

Resolution on principles and expectations for the appropriate use of personal information in facial recognition technology (2022)[6].

Recognizing that the ubiquity of means of surveillance, from the computerized archive of individuals personal data to the growing number of surveillance cameras, among others, inherently raises critical questions about the protection of personal data and ~~the~~ privacy, as rights of individuals which are a prerequisite for a functioning democratic society. The expansion and sophistication of information technology, along with the pervasiveness of networks and the Internet (e.g. connected devices, social medias, etc.), and the development of advanced biometric systems, high-definition video surveillance cameras, and precise geolocation tools, illustrate the need for a debate around the role of such technologies in our contemporary society. This pervasive reality forces us to reflect deeply on the linkages between collective security and the privacy rights of individuals and communities, in a context where technology is advancing by leaps and bounds and there is a risk that surveillance becomes a constant in everyday life. It is imperative that policies and regulations ensure that integrity and personal autonomy are not compromised on the altar of modern surveillance. These developments have transformed the way surveillance techniques are implemented, entailing in particular the unacceptable risk of constant and pervasive monitoring and tracking of individuals at mass scale in all public spaces;

Considering that public sector authorities should implement surveillance measures only when allowed by law, and as necessary and proportionate, it is essential that these measures are designed with a focus on minimal intrusion into the private lives of individuals. Public sector security strategies must be carefully calibrated to ensure effective protection without unduly transgressing the boundaries of personal privacy. Preserving the right to personal data and privacy is essential to preserve public trust, and to ensure that surveillance technologies and practices align with the ethical and legal values of a democratic society;

Recognizing that the use of emerging surveillance technologies or the development of new infrastructures likely to have the same effect (e.g. payment infrastructures) can pose significant risks to individuals' privacy and personal data, it is imperative to take a proactive and cautious approach. If in particular not designed in accordance with the principle of data protection by design and by default, technological innovations[7], while offering advanced tools for security, must also be critically evaluated in terms of their potential to infringe the right to the protection of privacy and personal data. Therefore, priority should be given to implementing robust protection measures that safeguard personal information from unauthorized exposure, misuse, or illicit access, thus ensuring respect for individual privacy;

Highlighting the fact that the development of technologies that comply with the principles and duties regarding the protection of personal data must involve a clear and in-depth

[6] 15.1.c.Resolution-on-Principles-and-Expectations-for-the-Appropriate-Use-of-Personal-Information-in-Facial-Recognition-Technolog.pdf (globalprivacyassembly.org)

[7] For example, Central Bank Digital Currency (CBDC) may also entail a risk of mass surveillance on economic transactions taking place via this digital currency.

understanding of the fundamental principles that underpin them. This is essential to ensure that its collection and processing is carried out in a transparent and accountable manner, with an unwavering commitment to integrity and confidentiality. A solid framework based on these principles must be established, which reinforces individuals' trust in the entities that handle their data, as well as ensuring that data management practices are aligned with the highest ethical and legal standards of privacy;

Recognizing that surveillance technology protocols must possess the necessary flexibility to address new challenges and developments in the surveillance system always remaining aligned with the fundamental principles of personal data protection. It is crucial that these protocols are dynamic and adaptable, allowing for continuous updating and improvement in the face of technological innovations and changing social contexts. At the same time, they must be firmly anchored in an unalterable commitment to data privacy and security, ensuring that each new implementation or adjustment is made with due consideration of individual rights and freedoms;

Taking into consideration the risks these technologies pose to personal data and privacy such as invasion of privacy, data breaches, misuse of information, deviation from the original purpose, psychological impact on individuals, data aggregation, potentially with inaccurate data or inferences, resulting in adverse consequences for individuals" is a risk, tracing of transactions, profiling, among others, Strict controls and mitigation measures are essential. These should be designed not only to prevent such risks, but also to provide effective remedies should they materialize. In any case, human dignity and autonomy must be preserved, ensuring that technology serves the well-being of society without compromising the core values of privacy and individual freedom. The ban of some uses of these technologies should also be considered, when they pose inacceptable risks on the fundamental rights of individuals or groups;

Considering the imperative need to mitigate the risks of invading privacy including via data protection safeguards in particular privacy by design in order to protect individuals, it is vital to implement a comprehensive framework of action that proactively addresses the vulnerabilities inherent in surveillance technologies (notably, cybersecurity risks), and there must be a constant commitment to risk assessment, the adoption of preventive measures, and the creation of rapid response systems to counter any threat to the privacy and security of personal data. This approach must be holistic and multidisciplinary, involving technology experts, policymakers, regulators and civil society, to ensure that the dignity and fundamental rights of every person are preserved as we move towards a technologically advanced future;

Emphasizing that compliance with data protection and privacy standards and principles is crucial for the responsible and reliable development and deployment of surveillance technologies, anywhere in the world, keeping their development and deployment proportionate and respectful of human rights. This is not only a matter of legal compliance, but also a fundamental pillar to build trust between individuals and the institutions that deploy such technologies.

Reaffirming the commitments in the GPA's 2023-25 Strategic Plan to maximize the voice of the Assembly in Digital Policy, enhance its role in wider digital policy debate at an international level, strengthen regulatory cooperation and work towards a regulatory environment with high standards of personal data protection and privacy that are clearly and consistently applied across the world;

Recognizing that when we talk about surveillance technologies, we must address not only the technical and legal issues, but also the ethical, social and cultural aspects related to privacy and surveillance, so collaboration is essential to achieve an appropriate balance between security and the protection of fundamental rights, it is in this context that we must **highlight** the importance of the following aspects:

- **Transparency and Accountability:** Data controllers must be transparent about the terms and standards they apply. This involves clearly setting out how they will process personal data and what they will do to demonstrate their responsibilities to individuals to comply with international, national, or sub-national instruments and standards.

- **Privacy Impact Assessment (PIA):** Implement PIA processes to assess the implications of surveillance technologies prior to adoption. This will help identify potential risks and design appropriate safeguards.
- **Education and Public Awareness:** Encourage education programs to inform the public about their rights in relation to privacy and surveillance technologies. Public awareness is critical to empowering people and ensuring they understand the risks and opportunities of these technologies.
- **International Cooperation:** Promote cooperation between policy makers and legislators to develop standards and practices that respect privacy and data protection. International collaboration is essential to address global surveillance-related challenges.
- **Biometric Data Protection:** Specifically consider the protection of biometric data, through technologies that process biometric data such as fingerprints, facial recognition, iris recognition technologies, hand geometry, retina recognition, voice recognition, vascular recognition and DNA. This data is particularly sensitive and requires additional security measures. Remote biometric identification in public spaces should be prohibited or at least restricted, according to different use cases.
- **Rights of Vulnerable Groups:** Ensure that surveillance technologies do not disproportionately affect vulnerable groups, such as ethnic minorities, people with disabilities, or marginalized communities.
- **Independent Audits:** Conduct periodic independent audits to assess the implementation and compliance with oversight policies. This ensures accountability and the correction of potential abuses.
- Oversight by independent authorities and meaningful right to redress should be in place.
- **Protection of Journalists and Human Rights Defenders:** Establish specific safeguards to protect journalists and human rights defenders from undue surveillance. These people play a crucial role in society and should be able to work without fear of reprisals.

The 46th Global Privacy Assembly (GPA) therefore adopts the following resolution on surveillance and protecting individuals' rights to privacy, and considers the following priorities:

- It is crucial to stress the importance of carefully assessing the necessity, proportionality, and minimization of data collection, ensuring that any surveillance measures are adequate, necessary and effective in relation to the objective being pursued;
- As recognized at international level, mass surveillance (the general and indiscriminate monitoring of the content of communications, for instance) should not be allowed, since in breach of the essence of human rights in particular the right to privacy and to the protection of personal data;
- Highlight the importance of guaranteeing sufficient legal bases for this type of processing, recalling in particular that the interference should be based as a rule on a legislative measure that it is sufficiently clear to provide foreseeability to citizens about its impact on them;
- Before implementing new surveillance technologies, it is essential to conduct comprehensive assessments that consider potential risks to personal data and privacy. These assessments should include purpose and objectives, accuracy and reliability, privacy and ethical considerations, cost-effectiveness, human factors and public perception;
- Facilitate the adoption of robust data protection measures, such as encryption, anonymization and secure storage of surveillance data, emphasizing the need for strict access controls and data retention limits to prevent unauthorized use or misuse of personal data;
- Surveillance technologies should be developed with privacy by design principles in mind which means incorporating privacy and data protection features into the design and architecture of the systems from the outset;
- Maintain public trust by providing clear information to individuals about the purpose, scope, and extent of surveillance activities, as well as how their data is collected, used, and shared;
- Foster collaboration between the GPA, its DPAs and other stakeholders to develop common privacy standards, policies and guidelines for the ethical and responsible use of surveillance technologies;
- Ensure that the development of privacy standards takes account of the intersection with other rights and freedoms (e.g. freedom of expression. freedom of assembly).
- Include collaboration with Data Protection Authorities such as regulatory sandbox initiatives in the process of adopting surveillance technologies to ensure that privacy rights are respected;
- Make sure that processing of personal data for national security and defense purposes are subject to independent and effective review and supervision under domestic legislation.
- Incentivize initiatives to educate the public about surveillance technologies, their privacy implications, and how to protect personal data;

- Invest in research and development to address the challenges and risks associated with surveillance technologies;
- Each data protection or privacy authority and other national or international research bodies to invest in training and capacity building to enhance knowledge and expertise in privacy protection and responsible surveillance practices to maintain the balance between the security needs and the protection of individuals' privacy;
- Ensure that the right to access, rectification, cancellation and opposition to the processing of personal data in surveillance databases is guaranteed, within reasonable legal limits, thereby allowing individuals to exercise their rights to informational self-determination, mainly in the deletion of their personal data when they are no longer necessary or relevant;
- Ensure that effective redress mechanisms for individuals are available to challenge misuse of their data or unwarranted surveillance;
- Impose strict restrictions on the secondary use of data collected through surveillance technologies to prevent profiling and discrimination;
- Conduct regular audits and reviews of surveillance technologies and practices to ensure compliance with data protection laws and regulations;
- The authorities justify the use of surveillance technologies for strictly necessary purposes related to national security or other purpose necessary to guarantee the fundamental rights and dignity of citizens and collectively; and
- Take into account the declarations and resolutions established by organizations and forums such as the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities and other GPA resolutions in the aspects related to mass surveillance.