42ND CLOSED SESSION OF THE GLOBAL PRIVACY ASSEMBLY

OCTOBER 2020

ADOPTED RESOLUTION ON FACIAL RECOGNITION TECHNOLOGY

***SPONSORS*:**

- Information Commissioner's Office, United Kingdom
- Office of the Australian Information Commissioner, Australia

***CO-SPONSORS*:**

- Agencia de Acceso a la Información Pública (AAIP), Argentina
- The Information and Data Protection Commissioner, (Komisioner për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale), Albania
- National Privacy Commission, The Philippines
- Office of the Privacy Commissioner of Canada
- Personal Information Protection Commission, Japan
- Préposé fédéral à la protection des données et à la transparence (PFPDT), Switzerland
- San Marino Autorità Garante per la protezione dei dati personali
- National Institute for Transparency, Access to Information and Personal Data Protection, Mexico
- Office of the Privacy Commissioner, New Zealand
- Commission nationale de l'informatique et des libertés, France
- National Commission for Informatics and Liberties, Burkina Faso

The 42nd Annual Closed Session of the Global Privacy Assembly

ACKNOWLEDGING that the capabilities of facial recognition technology are significant, and its potential applications could provide benefits to security and public safety;

HIGHLIGHTING that facial recognition technology has the capability to enable widespread surveillance, to be highly intrusive, provide biased results, and erode data protection, privacy and human rights, which in turn reduces trust and confidence in its use;

EMPHASIZING that facial recognition technology relies on sensitive biometric information that is unique and enduring, and that decisions made about individuals using these identifiers, potentially without their knowledge or consent, can lead to adverse consequences without adequate avenues for recourse;

NOTING that facial recognition technology may incorrectly identify or authenticate an individual or may fail to identify or authenticate an individual;

NOTING that public bodies, private organisations and civil society have expressed concern that the technology poses privacy, legal and ethical challenges that must be addressed;

RECOGNIZING that there are shared, widespread concerns about certain uses of facial recognition technology and its increased deployment in a number of applications and varied contexts including but not limited to:

- The live identification of individuals in public spaces for purposes of public safety or the prevention and detection of crime, by law enforcement bodies and other organisations;
- The use of live facial recognition in the fight against COVID-19, in identifying individuals displaying symptoms, or breaking quarantine rules;
- The identification of individuals by matching photographs to images held in databases compiled from sources such as social media;
- The capacity of facial recognition technology's use to evolve and be used in unforeseen ways or linked with other technological capabilities, in a manner that creates risk of harm to individuals and public confidence.

RECOGNISING that different uses of facial recognition pose different types and levels of risks and therefore require careful consideration in order to identify appropriate safeguards in each context and use;

CONCERNED that the respect of data protection and privacy rights are increasingly challenged by the rapid development of facial recognition technology, where large-scale datasets are often collated from a variety of publicly available and private sources, often without an individual's knowledge or consent, and made commercially available for use in new or unforeseen contexts;

CONCERNED that the widespread use of facial recognition can entail discriminatory effects and impact the ability to exercise certain other fundamental rights such as the freedom of expression and association;

RECOGNISING that in order to build and retain the trust and confidence of citizens, the potentially significant data protection and privacy risks to individuals, groups of individuals and society at large need to be identified and mitigated through adherence to relevant legal frameworks, establishment of technical and organisational safeguards and consideration of ethical concerns and human rights before facial recognition technology is deployed.

EMPHASISING the importance that development and implementation of those frameworks incorporate data protection and privacy principles, including requiring clearly defined purposes, a clear lawful basis, necessity and proportionality, fairness and transparency, individual rights and clear, accountable governance structures, before facial recognition technology is deployed;

RECALLING that the Global Privacy Assembly has previously identified the need to work towards global policy, standards and models and to ensure greater levels of regulatory cooperation to enhance the efficient prevention, detection, deterrence and remedy of data protection and privacy issues and to ensure consistency and predictability in the system of oversight in the data economy;

AFFIRMING the need for data protection and privacy enforcement authorities to coordinate their efforts to influence the development and implementation of those data protection and privacy approaches across the globe, and to take action where appropriate; and

REAFFIRMING the Resolution on Privacy by Design adopted by the 32nd Conference in 2010 in Jerusalem, the Resolution on Profiling adopted by the 35th Conference in 2013 in Warsaw, the Resolution on Big Data adopted by the 36th Conference in 2014 in Fort Balaclava and the Declaration on Ethics and Data Protection in Artificial Intelligence adopted by the 40th conference in Brussels.

Therefore the 42nd Global Privacy Assembly reiterates the importance of:

1. The principles of data protection and privacy by design in facial recognition technology development and use;
2. Necessity and proportionality principles, ensuring that facial recognition technology cannot be used where the purpose can reasonably be achieved by less intrusive means;
3. Transparency and accountability about the use of personal data and its governance in facial recognition applications, and applicable rights for individuals, including in provision of the technology to and their use by law enforcement agencies;
4. Requirements of fairness in processing personal data;
5. An ethical approach to the use of biometric data; and
6. Legal frameworks that are fit for purpose in regulating evolving technologies such as facial recognition technology.

The 42nd Global Privacy Assembly resolves to work together in 2020-21 to:

1. Focussing on the areas outlined above, consider in what circumstances facial recognition technology poses the greatest risk to data protection and privacy rights, and develop a set of agreed principles and expectations for the appropriate use of personal information in facial recognition technology, including recommending how the risks can be mitigated, to be adopted at the 43rd Global Privacy Assembly Closed Session;
2. Seek to promote the agreed principles above with a range of key external stakeholder groups to be identified, such as developers and users of facial recognition technology systems, to ensure innovative uses of facial recognition technology respect data protection and privacy by design obligations;
3. Request the International Enforcement Working Group and the Working Group on Ethics and Data Protection in Artificial Intelligence to deliver the work, taking account of the work carried out by other Working Groups of the conference where relevant and consulting with the stakeholder reference panel as appropriate.