Privacy International's statement for Informal Exchanges on Artificial Intelligence in the Military Domain, Session 7 - AI and Other Technologies
range of such convergences, including information and communication technologies

[CHECK AGAINST DELIVERY]

16 June 2026

Thank you Chair and distinguished panellists

Many AI-enabled systems used in the military domain rely on learned representations derived from data.

The shift we're facing is that it's no longer about traditional military intelligence data. It's all kinds and sources of data being used to create foundation and train tools to support military aims.

In this context, mass surveillance of public spaces online and offline via facial recognition technologies play a key role, a concern noted also in the UN Secretary-General report.

One aspect of this trend is the collection of facial images of targeted population in the context of occupation and military actions. For example, governments and occupying powers have been using AI to process biometric data for the purposes of routine identification and authentication, border crossing, and surveillance of public spaces and predictive risk assessment.

A second aspect is that facial recognition technology developed in civilian contexts are often repurposed in military contexts with significant human rights implications. For example, a private company Clearview AI scrapped millions of online images to build their facial recognition technology. Despite rulings by many national data protection authorities that this practice was not compliant with data protection laws, Clearview AI continue to offer its technologies including reportedly to militaries.

AI technologies applied to biometric data can exacerbate exclusion and reproduce racial, ethnic, gender, social class, and other inequalities.

The rapid deployment of AI technologies to process biometric data has not been met by commensurate changes at the level of law or policy. National regulatory and legal frameworks continue to lag behind and, where they do exist, they are rarely effectively enforced, unable to properly safeguard against the hazards and potential misuses of biometrics.

In 2021 the UN Counter-Terrorism Committee Executive Directorate, CTED, noted the inadequacy of national legal frameworks to regulate biometrics. Since then, little has changed despite the increase adoption of biometrics and the use of AI to process the data. And even attempts such as the EU AI Act to introduce prohibitions and limits to the use of AI for processing biometric data do not apply for military or defence purposes leaving this gap unaddressed.

Thank you, Chair.