Privacy International's statement for Informal Exchanges on Artificial Intelligence in the Military Domain, Session 1 - Opening Remarks and Scene Setting

[CHECK AGAINST DELIVERY]

15 June 2026

Chair, Excellencies, ladies and gentlemen

I speak on behalf of Privacy International. We are a non-governmental organisation that researches and advocates globally against government and corporate abuses of data and technology. We investigate how peoples' personal data is generated and exploited, and how it can be protected through legal and technological frameworks.

Our starting point is that to effectively regulate AI in the military domain requires to recognise privacy and data protection not as peripheral technical considerations, but as core human rights obligations integral to any meaningful regulatory framework.

Personal data is at the centre of the AI applications in the military domain.

It is no coincidence that the big tech companies which have built their business model on the exploitation of personal data of billions of users are now central to the AI services provided to militaries, which are seeking to leverage AI technologies. Similarly, it is no coincidence that tech-defence companies offering AI services to analyse personal data are thriving.

The centrality of personal data cuts across most AI applications in the military domain. Just to look specifically at AWS, what renders a weapon autonomous is the processing of vast amounts of personal data. The identification, selection and engagement of targets are heavily reliant on mass quantities of personal data to be trained, tested, improved, and deployed.

The same central role of data apply in other use of AI in military domain. In fact, the integration of data-intensive technologies is at the core of these technologies.

The deployment of AI in military domain leads to the uncontrolled fusion of civilian and military data. The data fed into those systems are no longer confined to traditional understandings of what constitutes military intelligence.

All personal data is now considered relevant for military purposes. Users' data from social media platforms are now feeding into war machines. The role of civilian data into conflict zones has been evident in both Ukraine and Gaza. In simple terms, anyone's personal data may end up building a lethal algorithm and we would all be oblivious to this. That is an important pull/push factor for Big-Tech companies to enter the defense sector. That is also why many of these companies took back previous promises not to build AI for conflict-related purposes.

Despite its centrality, the role of personal data is often an overlooked consideration in the regulatory discussions at national and international levels. For example, personal data is often processed without an adequate legal framework in place - especially in the military domain. As national data protection legislation –when it exists–often carves out from their scope of application data processing related to national security, defence and/or military. A similar blanket exclusion is contained in recent regional AI legislative initiatives, including the EU AI Act. As a result, the processing of personal data for most AI systems in the military domain takes place in a regulatory vacuum, despite the serious interference with the right to privacy and other human rights that it entails.

To be clear it is not only the right to privacy that is at stake here.

The assumption that the more the data the better the accuracy is flawed. In practice, large datasets often reproduce noise, bias, and contextual errors, increasing the likelihood of misidentification and unlawful targeting, while exposing individuals and communities to disproportionate surveillance. Recent examples suggest that feeding more data to a target recommendations tool can lead to exponential increase in potential targets, rather than precision and accuracy.

Yet, it is not only the often-lethal consequences of the reliance of personal data by AI in military domain to determine their actions that come into play.

The indiscriminate, unregulated processing of personal data is putting entire populations within and outside conflict under constant surveillance. The context of many current armed conflicts, including military occupation, is characterised by methods of mass surveillance, including automated checkpoints, constant facial recognition and video surveillance, and biometric ID systems whether as method of control from armed forces or in exchange of humanitarian aid.

By relying on generalised harvesting of data the AI systems support forms of mass surveillance that lead to serious violations of human rights, including freedoms of expression, peaceful assembly, and movement, as well as principle of non-discrimination and political participation.

If I were to make just one recommendation at the outset of this discussion, it is to ensure that ongoing international efforts to regulate AI in the military domain explicitly articulate state obligations to respect and protect privacy and personal data, recognizing that data driven technologies in military domain directly shape risks of harm and must be governed accordingly.

Thank you Chair.