



October 16, 2023

Letter addressed to representatives of the governments of Member States to the European Union.

Our organisations would like to bring to your attention the importance of protecting safety and security-enhancing technology products in the upcoming EU Artificial Intelligence Act (AI Act).

The **Security Industry Association (SIA)** is the leading trade association for global security solution providers representing over 1,400 manufacturers and systems integrators serving government, commercial and residential needs, many of which are headquartered and/or operating in the EU. **ASIS International** represents security and risk management practitioners around the world, including Europe's largest community of over 3,000 security professionals across public and private sectors. The **International Biometrics + Identity Association (IBIA)** is the leading international trade group representing the identification technology industry, advancing the adoption and responsible use of technologies for managing human identity to enhance security, privacy, productivity, and convenience for individuals, organisations, and governments.

We welcome the proposal for an Artificial Intelligence Act as a needed initiative, and our members fully support the EU's goal to develop a human-centric, ethical, trustworthy and technology-neutral framework for AI. Most recent innovations in products critical to our industries and professions stem from AI-driven technologies, enabling groundbreaking improvements to access control, screening/detection, premise security and related smart home and smart building systems for example, which provide greater protections to businesses and consumers, and bolster public safety.

Maintaining a technology-neutral approach to regulation, as intended by the Commission, is crucial to enable legitimate practices and technologies to continue to flourish in the EU. In our view, the most stringent requirements should apply to use-case specific and truly high-risk applications.

We are therefore concerned about the considerable expansion of prohibited technologies under the European Parliament's approach to Article 5 of the AI Act, often based on overly broad and vague terms. In particular, we are concerned about the following blanket bans:

1. Ban on 'real-time' remote biometric identification systems' in publicly accessible spaces.

This would unintendedly include, for example:

- **Border Control & Travel Facilitation:** In Europe and across the world, many travel document verification and airline-provided 'curb-to-gate' biometric programmes that provide security and streamline boarding experiences rely on systems requiring "one-to-many" comparison based on daily flight and travellers' data.
- **Accessibility:** Some biometric identification applications can provide increased and customised accessibility for disabled persons, that enhances their health and safety. For example, they can assist people suffering from blindness, memory loss or prosopagnosia (face blindness) by recognizing or distinguishing between friends and others.
- **Sports and Entertainment Venues:** Biometric identification technology is being rapidly adopted by major venues to enhance fan experiences, including streamlined entry and secure area access for pre-enrolled groups.

- Gaming Industry: Biometric identification technology is widely used by casinos for VIP recognition and enhanced customer service programs, voluntary problem gambler self-exclusion and enhanced security.
- Facility Security Screening: Biometric identification technology can enhance the capabilities of operators to screen those entering a facility against a limited list for a wide range of purposes that protect occupants, such as allowing access for those authorised, or flagging possible unauthorised entry, including where there have been specific threats of violence, or a protective judicial order involving a specific individual has been issued.
- Security Services: Biometric identification technologies enable ‘virtual doorman’ systems and enhance remote guarding services that improve security, economise staffing and provide convenience for occupants and visitors.

2. **Ban on ‘biometric categorisation systems,’ and systems that ‘infer emotions’ (in the workplace).**

As defined in the AI Act, both functions include analysis of non-personal data and behavioural information that is well outside of biometrics and distinct from identification.

While we support ruling out the categorisation of people for discriminatory *purposes*, there are beneficial AI technology applications performing a categorisation *function* that cannot be overlooked, many of them crucial for the protection of health and safety of people. For example, categorisation using face classification technology has proven effective for determining the age of children accessing content online, detecting deepfakes and fighting the dissemination of child sexual abuse material. In other categorisation applications, today’s video and sensor analytics in security systems are capable of detecting, classifying and immediately reporting anomalies in human behaviour where an emergency response might be needed (i.e. detecting in video when an individual has slipped, fallen and needs assistance). Similarly, images can be grouped and sorted by physical characteristics to facilitate safety and efficiency improvements, incident investigations and other functions that dramatically improve business operations and occupant safety. This proposal could even prohibit AI systems that are used to detect bias in other AI systems, and thus have a clearly positive purpose.

Regarding systems that ‘infer emotions’, there are many beneficial AI technologies that could be interpreted as such and thus could be banned, from voice analytics that detect if there is loud shouting indicating an emergency where response is needed, to cameras that can identify whether a driver is drowsy and provide an alert. Such AI systems are safety relevant and should not be prohibited.

3. **Ban on any analysis of recorded footage using ‘post’ remote biometric identification systems, without *pre-judicial* authorisation** (an exception only applicable to law enforcement despite the larger scope of the prohibition). Such a prohibition will harm safety and security in many ways, including:

- Analysis of CCTV Recordings: Limiting the ability of security staff to conduct post-event safety or security investigations, where there was an accident, a missing person or other situation where use of the technology to analyse recorded footage could be essential to determining key facts.
- Emergency Response: Limiting the ability of responders to rapidly pinpoint and sort images in recorded video footage to, for example, determine which individuals have

escaped (or remain in) a building where there is a safety issue such as a fire, etc. or active threat.

- **Law Enforcement Investigations:** Depriving law enforcement authorities of key capabilities to solve serious crime, protect victims and quickly address terrorist threats. It would do so by impeding use of tools yielding “leads” on the identity of an unknown person of interest at the starting point of an investigation or response to an emergency, before information that might be necessary for ‘pre-judicial authorisation’ is available. The ability to act quickly is crucial to successful use of tools such as Interpol’s facial recognition system, which has helped identify over 1500 criminals, terrorists, fugitives, persons of interest and missing persons since it was launched in 2016.¹

We note that neither the Commission nor Member States proposed similar prohibitions in their versions of the Act despite comprehensive risk analysis. The Parliament has not proposed evidence that sufficiently back these far-reaching proposals for regulation.

The original objective of Article 5(1), proposed by the Commission and amended by the Council, was to prohibit potential forms of government mass surveillance in the EU, which is commendable. We believe this can be accomplished by imposing strict conditions on ‘real-time remote biometric identification systems’ in publicly accessible spaces for law enforcement purposes – without impacting unrelated private sector applications where biometric identification systems are already subject to specific safeguards under the General Data Protection Regulation (GDPR).

We strongly encourage an approach to AI regulation in which prohibitions are limited to the specific, harmful use cases of AI systems, whilst other practices are subject to the AI Act’s transparency or high-risk requirements. As technology itself is inherently neither good nor bad, the context and purpose for its use should be the key considerations.

For these reasons, on behalf of SIA and our members, we urge you to support the adoption of the Council’s approach to Article 5 of the AI Act. Otherwise, Member States could be left without many key tools which greatly improve their capacity to ensure their citizens experience a secure environment which protects their rights to the utmost degree, without privileging certain fundamental principles at the expense of others. Moreover, these prohibitions do not only concern security; it would be damaging to the single market if the prohibitions were to be interpreted in a manner which limits the ability of EU developers and providers of innovative AI-driven technologies to compete.

We stand ready to provide any further information or assistance you may need as you work to finalise this important legislation.

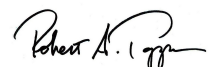
Kind regards,



Don Erickson
Chief Executive Officer
Security Industry Association
www.securityindustry.org



Peter O’Neil
Chief Executive Officer
ASIS International
www.asisonline.org



Robert Tappan
Managing Director
International Biometrics +
Identity Association
www.ibia.org

¹ <https://www.interpol.int/How-we-work/Forensics/Facial-Recognition>