BSIA White Paper

Artificial Intelligence - a European Approach
12 June 2020

Summary

The British Security Industry Association (BSIA) welcomes the European Commission's White Paper, *Artificial Intelligence – A European Approach to Excellence and Trust (COM(2020)65)*. As the United Kingdom's leading trade body representative of the private security industry, in this paper the BSIA focuses only on the use of Artificial Intelligence (AI) systems in the domain of security and law enforcement.

The BSIA believes that the seven key requirements developed in the European Commission's "Ethics Guidelines for Trustworthy AI" are useful guiding principles for building trust in AI and assuring compliance with fundamental rights. We support the idea that the introduction of legal and non-legal measures for "high-risk" AI applications, as outlined in the White Paper, can be suitable to address these principles. We however recall that a clear definition of these applications is necessary to guarantee harmonised implementation in the Member States and legal certainty for developers, manufacturers, service providers (installers and monitoring centres) and end-users.

The BSIA does not support a moratorium against remote biometric identification systems, such as facial recognition. The BSIA believes that such technologies can add considerable value to enhanced public security and law enforcement, and that their use should be allowed in public spaces based on a risk and impact assessment under adequate human oversight.

Human autonomy and oversight are key for the overall goal of human-centric, lawful, ethical, and robust AI. To reach that goal, every stakeholder in the chain – developers, manufacturers, service providers, end-users, testers, procurers – need to be empowered to preserve human autonomy by means of curricula and qualifications. The BSIA believes that for specific "high-risk" use-cases, the Commission should consider making certain qualification and licensing mandatory for developers, end-users and testers.

At the same time, it is important to keep financial and administrative burden for end-users as low as possible in order to ensure uptake of AI. This applies to liability frameworks as much as for conformity assessments and voluntary labelling. Support must be considered for SMEs.

Building trust in AI

The European Commission's White Paper, *Artificial Intelligence – A European Approach to Excellence and Trust (COM(2020)65)* correctly states that "trustworthiness is a prerequisite for its uptake". AI must, through the system's entire lifecycle, be lawful, ethical, and robust in order to guarantee compliance with fundamental rights and to build trust in AI. To live up to that goal, The BSIA believes that the seven key requirements developed in the "Ethics Guidelines for Trustworthy AI", published

by the European Commission's High-Level Expert Group on Artificial Intelligence, should be guiding principles for legal and non-legal actions:

1. Human agency and oversight;
2. Technical robustness and safety;
3. Privacy and data governance;
4. Transparency;
5. Diversity, non-discrimination and fairness;
6. Societal and environmental wellbeing;
7. Accountability.

These can ensure that a European approach to AI follows a human-centric approach in the sense that AI brings value to European businesses, workers and citizens, while respecting fundamental rights, human autonomy and decision-making.

Regulation of "high-risk" AI applications

The BSIA believes that the requirements that are considered by the European Commission for "high-risk" AI applications can be suitable to address these guiding principles:

• Training data, set in place by adequately skilled developers, is crucial for the lawful, ethical, and robust functioning of AI systems;

• Data and record-keeping as well as transparency ensure adherence to data protection laws and knowledge about when and under what circumstances AI is used – supporting public acceptance and legal certainty;

• Adequately skilled developers, service providers, end-users and testers must guarantee human agency and autonomy;

• Technical robustness is key to ensure cyber and physical resilience and security throughout the value chain.

The BSIA further supports the risk-based approach proposed by the European Commission when defining "high-risk" AI applications. In doing this, any future legal instrument will have to be very clear and unambiguous as to what "high-risk" AI applications mean and cover. Legal certainty will be a must, to leave no room for a different interpretation among EU Member States that could lead to distortions of competition or other legal issues.

The BSIA urges the European Commission to consider that AI applications can be inappropriately used for malicious and/or unethical purposes such as gender or racial profiling and this must be legislated against. Not only is technical robustness important, but also physical protection and human oversight. Security and fallback plans, constant human agency and oversight by qualified, if needed licensed and vetted staff, are key for the operation of "high-risk" AI solutions – particularly in specific high-risk applications such as access control and monitoring of Critical Infrastructure and public spaces. Private security can, with highly qualified and adequately licensed personnel under

oversight of law enforcement, ensure an appropriate use and protection of these technologies depending on sectoral legislation on a national level.

Depending on the application, specific human oversight measures may be a mandatory requirement for the usage of AI systems. The Ethics Guidelines on Trustworthy AI provide a useful overview of different approaches (human-in-the-loop, human-on-the-loop, human-in-command – see page 16).

Negative consequences of a moratorium on facial recognition systems

The BSIA believes that the use of remote biometric identification systems, such as facial recognition, should be allowed in public spaces if they can bring considerable added value to public safety and security, and where their use is correctly guided by an ethical and unbiased judgement. The BSIA strongly objects to a moratorium on these tools based on concerns about their possible misuse only and stands ready to contribute to a further debate on specific measures for remote biometric identification systems as announced in the White Paper.

A moratorium on facial recognition systems would negatively impact investment to improve their accuracy, effectiveness, efficiency and testing. It would slow down the pace of technology innovation, halt improvements already made, and leave the market to other countries instead of establishing a European, human-centric, leadership in these technologies.

Further, a moratorium would have negative consequences for the safety and security of European citizens, as it would pre-emptively deprive law enforcement of tools that can bring considerable added value in fighting crime when used alongside human oversight and intelligence while strictly complying with data protection and privacy legislation. Facial recognition can be critical to enhance security and capabilities of solutions like video surveillance, access control and identity management systems – especially at Critical Infrastructure.

Use-cases of remote biometric identification systems

When deploying remote biometric identification systems only in certain cases and specific circumstances, it is not about nationwide surveillance of citizens, but a targeted search for criminals and terrorists at particularly vulnerable locations. Using these techniques could, for example, help track down criminals and terrorist like Anis Amri, who killed twelve people in a terrorist attack in Berlin in December 2016 and fled via transport hubs in the Netherlands, Belgium and France to Italy. The automated comparison of video images with police databases, in which photos of criminals and wanted people are stored, is not comparable with the use of systems for which millions of photos of uncontested citizens are stored. Also, the alternatives to a ban would be far slower and prone to errors, e.g., when officers have to manually go through large quantities of videos and images of police databases. The BSIA adds that AI can likewise counterbalance (unconscious) human social biases and discriminatory patterns if adequately programmed.

The BSIA also stresses that there are use-cases of facial recognition, which do not come with a higher threat to fundamental rights than other applications that the Commission may consider being “high-risk” applications. For example, when it is used in verification processes to help verify a person is who they claim to be (e.g. in banking, access and border control), individuals have consented to or are required to prove their identities without a negative impact on privacy, if the requirements are fulfilled as lined-out in the White Paper.

Risk and impact-based approach for the use of remote biometric identification systems

However, it is important to conduct privacy impact and risk assessments before using remote biometric identification systems in public spaces. The use of a surveillance camera system must always be for a specified purpose, which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

When using such AI technologies, their added value and expected impact must be clear. Depending on the mission and location, AI technologies, physical intervention, and the blending of the two, through "augmented security" and mutual enhancement, must be considered in a risk and impact assessment. On-site law enforcement personnel or private security officers can often deliver better added value, e.g. by means of behavioural detection techniques or by being able to react and, if necessary, intervene directly on the spot – possibly supported by AI technologies in "augmented security" solutions. The deployment of surveillance technologies and/or physical guarding/surveillance must always fulfil the objectives of a mission under careful consideration of data protection, privacy and fundamental human rights.

Further, there must be legitimate interest to use remote biometric identification tools in public spaces based on a risk assessment process and an evaluation of physical and technological solutions that properly respond to the risk level. This does not only account for mass transportation hubs like airports and train stations, but also to public spaces which are often used during leisure activities, attract a critical mass of visitors, and represent so-called "soft targets" for terrorist attacks – including large concert halls and football stadiums for instance. The BSIA stresses that the lack of a past, real-life incident, for example of a terrorist attack, should not be an argument to dismiss the possible deployment of facial recognition technology. For example, only because an attack on a large cruise ship has not been carried out (yet), it does not mean that terrorists may not consider such a scenario in the future – which may make deployment of remote biometric identification systems at large cruise ship terminals under certain circumstances, such as heightened terrorist threat levels, useful.

Skills development as a game-changer: the importance of human oversight

In addition to this impact and risk-based approach, The BSIA stresses the relevance of human autonomy and oversight over AI and in particular remote biometric identification tools. Human review and, if needed, intervention, is crucial to ensure that any decision made by AI tools does not violate civil rights. Technologies like facial recognition should not be used to make fully automated, final decisions. Human autonomy, supervision and review of facial recognition results must be used to ensure rights are not violated. The Ethics Guidelines for Trustworthy AI provide an excellent overview of the different approaches of human oversight (human-in-the-loop, human-on-the-loop, human-in-command).

Skills are the very basis of human autonomy. To that end, those conducting human oversight of AI operations need to have adequate training, skills and qualifications. End-Users should be empowered through dedicated curricula and qualifications to reasonably self-assess or challenge the system.

The White Paper falls short in this regard as it only refers to providing curricula for developers. AI skills strategies are required along the entire value chain (developers, procurers, service providers, end-users and testers) based on sectoral needs, taking account of STEM and non-STEM skills, to ensure a human-centric AI approach. For specific high-risk applications, curricula and a licensing framework based on formal qualifications should be considered, if necessary, including vetting, for developers, service providers, end-users (including private security) and testers.

Close cooperation with sectoral Social Partners is crucial for the development of curricula to guarantee that qualifications respond to market needs and the specific use-cases of AI in different sectors. To support, a range of disciplines should be considered to be involved in the development of curricula, including ethics experts, neuroscientists, psychologists and sociologists. As the Ethics Guidelines for Trustworthy AI recommend, teams should not only be diverse in terms of gender, culture, age, but also in terms of professional backgrounds and skill sets.

The BSIA recalls the importance of seeing respect of law, ethics, technical robustness, safety and security of AI as a chain. Each link, from developers to manufacturers to service providers and end-users, needs to act, and interact, responsibly in order to maintain integrity of the system and a human-centric approach. To do that, each actor needs to be empowered by the right skills-set.

Avoid burden in liability rules and conformity assessments

While it is important to build trust in AI through different mandatory requirements as outlined in the White Paper, regulators should not lose sight of facilitated uptake of AI solutions by end-users.

The BSIA believes that the current EU legislative framework for liability should be amended to better cover the risks engendered by certain AI applications and that legal certainty on victim rights and liability is key. End-users should however only be held liable if they are best suited to respond and entitled to autonomously intervene in AI decisions. Developers carry a particular responsibility, as they largely define AI behaviour and learning. Producers must ensure that all products put on the market are safe throughout their lifecycle. Again, human oversight, traceability, skills, and, if necessary, licensing, are key at all stages of the value chain.

Furthermore, compliance assessment must have harmonised standards across countries to not leave gaps. To ensure AI uptake, financial and administrative burdens to end-users need to be as low as possible. Investments must be made in testing infrastructure and support structures are needed for businesses, with particular focus on SMEs. For example, predefined risk assessments and standard scenarios exist to facilitate the uptake of drone operations in Europe. The BSIA believes that similar solutions should be considered for the use of AI.

Regarding voluntary labelling schemes, any labelling system must respond to societal and industry needs to ensure uptake by businesses. In the light of technological development, the standardisation process must be efficient, flexible and cost effective. Participation of all relevant stakeholders is crucial. Investments must be made in the promotion of standards among industry and lawmakers - if of added value also for the uptake in laws, procurement, and contracts. Labelling should be complemented by accountability as well as review and redress mechanisms.

About the BSIA:

The British Security Industry Association (BSIA) is the trade association for the professional security industry in the UK.

Our members are responsible for more than 70% of privately provided UK security products and services (by turnover) including the manufacture, distribution and installation of electronic and physical security equipment and the provision of security guarding and consultancy services. Our members are industry professionals ranging in size from global companies to small and medium enterprises, offering quality products and services to a vast spectrum of end-users.

Our mission and vision

The BSIA is the voice of the professional security industry, supporting and encouraging excellence; educating the marketplace on the value of quality and professional security; and creating an environment in which to flourish.

BSIA Membership is the symbol of quality and professionalism in the security industry.

Press contact: Andrew Cooper Head of Communications

BSIA Ltd
Anbrian House, 1 The Tything,
Worcester,
WR1 1HD
ENGLAND
UNITED KINGDOM