October 2021
APPG AI Evidence Meeting

BIG INNOVATION CENTRE

National Security:
Regulation of AI-driven Live Facial Recognition Technologies

PARLIAMENTARY BRIEF

National Security: Regulation of AI-driven live facial recognition technologies (Live Facial Recognition) *is a* Parliamentary Brief based upon the All-Party Parliamentary Group on Artificial Intelligence (APPG AI) Evidence Meeting held online on the 11th October 2021.

This APPG AI is co-Chaired by **Stephen Metcalfe MP** and **Lord Clement-Jones CBE**.

We would like to express our appreciation to the following people for their oral evidence:

- **Professor Ivan Tyukin,** Head of the Visual Intelligence Lab, **University of Leicester**
- **Lindsey Chiswick,** Director of Intelligence, **Metropolitan Police Service (MPS)**
- **Dr Peter Wagget,** BSI Chair, **IST/44 Biometrics Committee**
- **Pauline Norstrom,** Honorary Member**, British Security Industry Association (BSIA)**
- **Lucy Holmes,** Managing Director**, Omni Telemetry** and Associate Partner**, 87 Holdings Ltd.**
- **John Buyers,** Head of Commercial**, Osborne Clarke**

Big Innovation Centre is the appointed Secretariat for APPG AI

- CEO, **Professor Birgitte Andersen**
- Rapporteur: **Dr Désirée Remmert**

The video recording of the Evidence Meeting can be found on our websites.

www.biginnovationcentre.com | Email: info@biginnovationcentre.com | @BigInnovCentre

https://uk.bicpavilion.com/about/appg-artificial-intelligence |
Email: appg@biginnovationcentre.com | @APPG_AI

PARLIAMENTARY BRIEF

National Security:
Regulation of AI-driven Live Facial Recognition Technologies

All Party Parliamentary Group on
Artificial Intelligence

APPG AI Sponsors

The Group supporters – British Standards Institution, Capita, CMS Cameron McKenna Nabarro Olswang, Deloitte, Dufrain, Omni, Osborne Clarke, PwC, and Rialto – enable us to raise the ambition of what we can achieve.

Contents

1. Introduction

Having focused on the ethical and societal implications of the use of facial and emotion recognition systems in our 2020 evidence meeting “Face and emotion recognition: How can regulation protect citizens and their privacy?”, we now look into the deployment of these technologies in the context of national security.

At the upcoming APPG AI evidence meeting, we will discuss which policies and regulation are necessary to guarantee the secure deployment of Live Facial Recognition to improve the safety of citizens, institutions, and the economy without exacerbating existing socio-economic and ethnic divides or infringing on individuals' privacy rights. In this context, we would like to draw on recent national and international publications on this issue such as the Information Commissioner’s Opinion: The use of live facial recognition technology in public places and the EU Commission's Regulatory Framework Proposal on Artificial Intelligence which might be helpful in developing the regulation of data-driven surveillance technologies in the UK.

List of panellists:

- **Professor Ivan Tyukin,** Head of the Visual Intelligence Lab, **University of Leicester**
- **Lindsey Chiswick,** Director of Intelligence, **Metropolitan Police Service (MPS)**
- **Dr Peter Wagget, The British Standards Institution** (BSI) Chair, **IST/44 Biometrics Committee**
- **Pauline Norstrom,** Honorary Member**, British Security Industry Association (BSIA)**
- **Lucy Holmes,** Managing Director**, Omni Telemetry** and Associate Partner**, 87 Holdings Ltd.**
- **John Buyers,** Head of Commercial**, Osborne Clarke**

This meeting was chaired by co-Chair **Lord Clement-Jones CBE. C**o-Chair **Stephen Metcalfe MP** sent this apologies for this meeting.

Parliament has appointed Big Innovation Centre as the **Secretariat of the APPG AI**, led by **Professor Birgitte Andersen (CEO)**. The Project Manager and Rapporteur for the APPG AI is **Dr Désirée Remmert**.

2. Recommendations for policymakers

Our expert speakers at the APPG AI evidence meeting suggest that regulation governing the deployment of Facial Recognition Technology and Live Facial Recognition must guarantee the **safeguarding of training data and AI models**, it should provide **ethical instructions and a code of conduct for the developers** of these technologies, and encourage **public trust and the willingness to cooperate** in the deployment of face recognition technologies for national security. Further, it should guarantee **technical oversight and accountability for errors** in the deployment of Facial Recognition Technology and Live Facial Recognition. Lastly, granted that the **state sponsored and commercial use of face recognition technologies raises similar ethical concerns** in relation to human rights and privacy, it has been recommended that government considers a **streamlined and consistent regulatory approach** to the deployment of Facial Recognition Technology and Live Facial Recognition.

Our expert speakers at the meeting agree that **Live Facial Recognition can provide an important contribution to National Security if deployed in a safe and transparent manner** and if it is **supported by the public**. However, to guarantee the reliability of Live Facial Recognition systems, it must be ensured that they are trained with **representative data**, that they are **subjected to regular auditing**, and that **public trust** in these technologies is secured by conveying **transparent information about their application and the usage of the data they generate**.

Pauline Norstrom, Honorary Member of the British Security Industry Association, stresses that **most publicly accessible places in the UK are surveilled by privately owned cameras**. The images captured by these cameras would be analysed by a facial recognition system, either through an **inbuilt AI-driven software** or in a **cloud**. Many of these cameras would even have an Live Facial Recognition capability which, however, would rarely be switched on.

Lindsey Chiswick, Director of Intelligence at the Metropolitan Police Service exlplains that **Live Facial Recognition helps spotting "those posing a risk of harm by monitoring facial images of people within a zone of recognition**. Images from specially located cameras are searched against a watchlist of images of people who are wanted, or based on intelligence are suspected of posing a risk of harm to themselves or others. **Where the Live Facial Recognition system identifies a potential match, the system flags an alert to an officer who considers that alert and makes a decision on whether any further action is required. If there is no alert, the biometric data is immediately and permanently deleted.**" This technology, she stresses, has a critical role to play in fighting crime and ensuring public safety in the city.

Professor Ivan Tyukin, Head of the Visual Intelligence Lab, University of Leicester, recognises the benefits of these technologies in the area of National Security but also alerts to the dangers

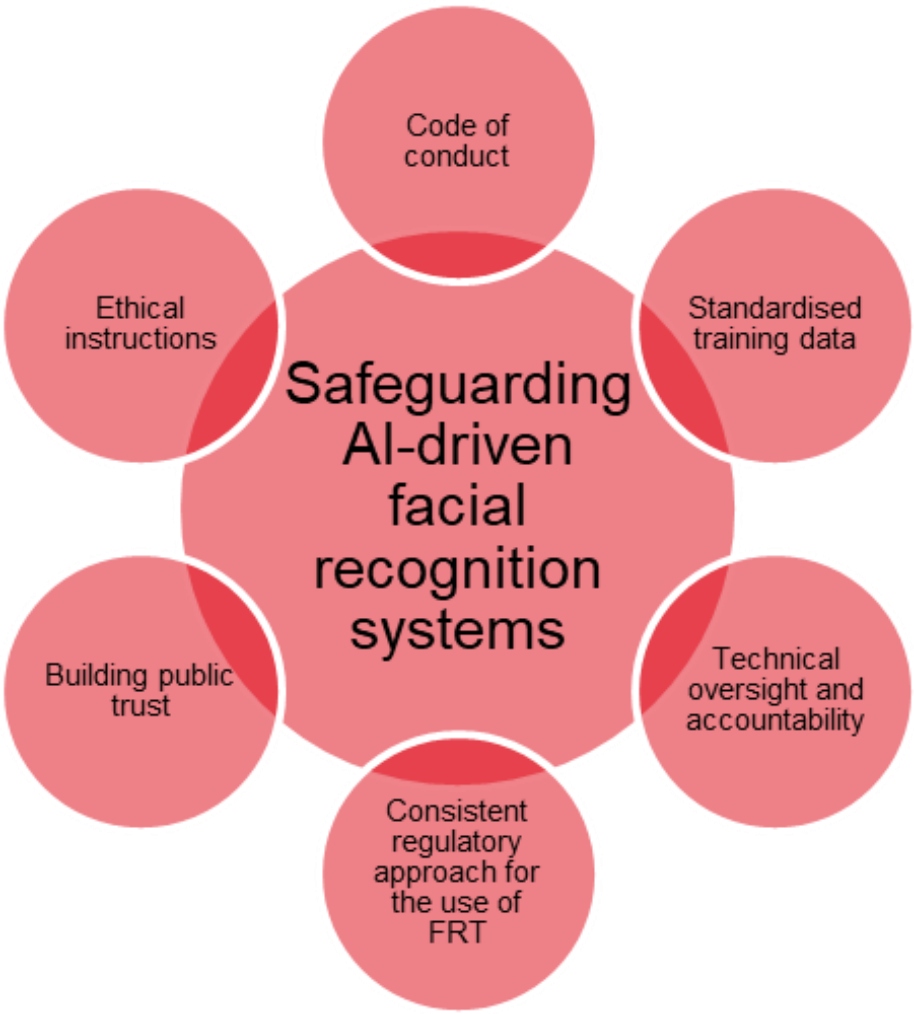
that the widespread and still relatively unregulated deployment of AI-driven face recognition systems might imply in certain contexts. One instability that data-driven systems are prone to, he stresses, is **adversial data**. “Adversarial data”, Tyukin explains, “are data which were **modified to closely resemble legitimate objects of interest** so that a human observer may not be able to identify that they are dealing with inappropriate data. When passed to a relevant data-driven AI, this data **evoke incorrect responses**.”

Further, he notes, AI-driven systems such as Live Facial Recognition can be prone to “**backdoor attacks**”. This means that an attacker gains an **access to data-driven AI or to its production pipelines to manipulate the system**. “Data poisoning”, where an attacker modifies training data to generate “wrong” decisions by the AI system which then can be exploited by the attacker constitutes a typical “backdoor attack.” Another common mechanism used to manipulate the decisions generated by these technologies are **“stealth attacks**” where attackers plant faults in the model (neuron replacement etc.). For this reason, Tuykin continues, regulation must ensure the **safeguarding of the data and AI models**, it must provide **ethical instructions and a code of conduct for AI developers**, **build public trust** and **willingness to cooperate and ensure accountability for errors** in the deployment of Facial Recognition Technology and Live Facial Recognition.

John Buyers, Head of Commercial at Osborne Clarke, stresses that policymakers should **not only focus on state-sponsored surveillance use cases** of this technology but should also pay attention to how they are **permeating products and services provided by the private sector**. He notest that “the UK regulatory position is horrendously complicated and filled with overlapping regulation” and that ”the regulation of state sponsored Automated Facial Recognition is completely different to private use”. Further, Buyers criticises, that a DCMS consultation led review into the role of data in the UK society would overlook the fact that **regulation is bifurcated into private use as well as state sponsored use**. That is, **the private and commercial use of Automated Facial Recognition raises similar ethical concerns in relation to human rights and privacy**. For these reasons, he continues, it should be regulated. “However, when used properly, it can be a significant aid to convenience and security. The National Strategy for AI does not cover this topic at all”. Accordingly, he suggests “a **streamlined approach which will provide consistent guidance for both the private users of this technology, and those that are sponsored by the state.**”

In sum, our expert speakers suggest that regulation governing the deployment of Facial Recognition Technology and Live Facial Recognition must guarantee the **safeguarding of training data and AI models**, it should provide **ethical instructions and a code of conduct for the developers** of these technologies and encourage **public trust and the willingness to cooperate** in the deployment of face recognition technologies for national security. It further should guarantee **technical oversight and accountability for errors** in the deployment of Facial Recognition Technology and Live Facial Recognition. Lastly, granted that the **state sposored and commercial use of face recognition technologies raises similar ethical concerns** in relation to human rights and privacy, it has been recommended that government considers a **streamlined and consistent regulatory approach** to the deployment of Facial Recognition Technology and Live Facial Recognition.

Illustration: Safeguarding AI-driven facial recognition systems



3. Evidence statements

Professor Ivan Tyukin, Head of the Visual Intelligence Lab, University of Leicester

On potential dangers of using data-driven technologies in national security

Ivan Tyukin is a Professor of Applied Mathematics at Leicester. As a Turing AI Fellow he works on Adaptive, Robust, and Resilient, is a member of the UKRI Trustworthy Autonomous Systems Verifiability node. He leads Visual Intelligence Lab, Next Generation digital intelligent systems facility at Space Park Leicester (a part of £13M Research England METEOR programme), and is an Editor of Communications in Nonlinear Science and Numerical Simulation.

Evidence

Unlike traditional systems built on knowledge and understanding of the problem, Data-driven AI built with Machine Learning are designed directly from data.

Despite these systems show great performance, a mounting body of literature suggests [1-5] that they may, unfortunately, be prone to instabilities. Under some appropriate conditions these instabilities are in fact expected [2-5]. Examples of data-driven AI instabilities are adversarial data [6]. **Adversarial data** are data which were modified to closely resemble legitimate objects of interest so that a human observer may not be able to identify that they

are dealing with inappropriate data. When passed to a relevant data-driven AI, this data evoke incorrect responses.

Adversarial data may include images with purposefully designed small perturbations added to an image [7], a purposefully designed makeup [8], different haircuts, alterations of geometry, or a combination of all these.

The other issue are backdoor attacks [9]. Backdoor attacks emerge when an attacker gains an access to data-driven AI or to its production pipelines. A compromised AI operates as expected most of the time. However, for a special input known to the attacker, the AI produces decisions which the attacker wants to trigger.

Several mechanisms implementing backdoor attacks have been revealed to date. One is the **data poisoning** whereby an attacker accesses and modifies AI's training data. That way "wrong" decisions will be learned and exploited by the attacker. The other mechanisms are **"stealth" attacks** whereby an attacker physically plants a fault (replaces a single neuron) into the model [4,10]. Alarmingly these vulnerabilities are difficult to spot from input-output observations [4,10]. These latter attacks are markedly different from **trajan attacks** in which a large portion of AI may have to be changed [11].

Vulnerabilities which I mentioned highlight pathways to safeguard against them.

Safeguarding Data. Data used to develop AI models for security are to be viewed as security assets. Creation and accessing this data must be regulated. Otherwise, risks of adversarial attacks are high.

Safeguarding AI. AI models used in security-sensitive areas must be rigorously tested for instabilities and planted faults. Testing for these must be a part of their "roadworthy" status. Safety and robustness standards need to be developed. Access to operational AI used in security is to be strictly regulated.

Introduction of AI developers' Ethics. Professional integrity and good character of AI developers and users are important safety factors. An appropriate code of conduct needs to be developed and used throughout the industry. In the short term, and to initiate this movement, it may be useful to consier engaging with ORBIT – observatory for responsible research and innovation in ICT https://www.orbit-rri.org/about/meet-the-team/

Citizen's understanding and cooperation are important to prevent a never-ending arms race by using makeup or cloth patterns preventing face recognition systems to detect a face (please see [13] for some examples of such camouflaging makeup and facial paint). Open public consultation is needed to establish acceptable limits for using such technologies.

Assigning responsibility for errors and dealing with errors. If things go wrong, determining who is responsible for errors is absolutely important. Is this always a developer, a user, or is this decided on a case-by-case basis? There must be mechanisms enabling to correct errors

immediately, and at scale if needed, after they are identified. Some research has already been done in this area [12], but there may be a need to do more work focused e.g. on live face recognition and related areas.

These are the areas where legislation and regulation are needed and where they can be put in place before anything goes wrong.

References

1. Yang, L., Song, Q. & Wu, Y. Attacks on state-of-the-art face recognition using attentional adversarial attack generative network. Multimed Tools Appl 80, 855–875 (2021). https://doi.org/10.1007/s11042-020-09604-z

2. Antun, V., Renna, F., Poon, C., Adcock, B., Hansen, A.C. On instabilities of deep learning in image reconstruction and the potential costs of AI. PNAS 117 (48) 30088-30095 (2020); https://doi.org/10.1073/pnas.1907377117

3. Shafahi, A., Huang, W.R., Studer, C., Feizi, S., Goldstein, T. Are adversarial examples inevitable?. arXiv preprint arXiv:1809.02104(2018).

4. Tyukin, I. Y., Higham, D. J., and Gorban, A. N. On adversarial examples and stealth attacks in artificial intelligence systems. In *2020 International Joint Conference on Neural Networks (IJCNN)* (pp. 1-6). (2020) https://arxiv.org/abs/2004.04479

5. Bastounis, A., Hansen, A.C., Higham, D.J., Tyukin, I.Y., Vlačić, V. Deep Learning: What Could Go Wrong. SIAM News (2021). https://sinews.siam.org/Details-Page/deep-learning-what-could-go-wrong

6. X. Yuan, P. He, Q. Zhu and X. Li, "Adversarial Examples: Attacks and Defenses for Deep Learning," in IEEE Transactions on Neural Networks and Learning Systems, vol. 30, no. 9, pp. 2805-2824, Sept. 2019, doi: 10.1109/TNNLS.2018.2886017.

7. Goodfellow, I. J., Shlens, J., Szegedy, C. Explaining and harnessing adversarial examples. arXiv preprint arXiv:1412.6572 (2014).

8. Z. Zhu, Y. Lu and C. Chiang, "Generating Adversarial Examples By Makeup Attacks on Face Recognition," 2019 IEEE International Conference on Image Processing (ICIP), 2019, pp. 2516-2520, doi: 10.1109/ICIP.2019.8803269.

9. Gao, Y., Doan B.G., Zhang, Z., Ma, S., Zhang, J., Fu, A., Nepal, S., Kim, H. Backdoor attacks and countermeasures on deep learning: A comprehensive review. *arXiv preprint arXiv:2007.10760* (2020).

10. Tyukin, I.Y., Higham, D.J., Woldegeorgis, E. and Gorban, A.N.. The Feasibility and Inevitability of Stealth Attacks. *arXiv preprint arXiv:2106.13997* (2021).

11. Y. Liu, S. Ma, Y. Aafer, W.-C. Lee, J. Zhai, W. Wang, and X. Zhang. Trojaning attack on neural networks. In Network and Distributed System Security Symposium (NDSS) (2018).

12. Gorban, A.N., Golubkov, A., Grechuk, B., Mirkes, E.M. and Tyukin, I.Y. Correction of AI systems by linear discriminants: Probabilistic foundations. *Information Sciences*, *466*, pp.303-322 (2018)

13. https://www.theguardian.com/world/2020/feb/01/privacy-campaigners-dazzle-camouflage-met-police-surveillance

Lindsey Chiswick, Director of Intelligence, Metropolitan Police Service (MPS)

The Metropolitan Police Service (Met) submission of evidence to the All-Party Parliamentary Group on Live Facial Recognition (Live Facial Recognition) offers a law enforcement perspective in the context of crime prevention. The evidence:

- Outlines how the Met uses Live Facial Recognition technology;
- Describes the benefits that Live Facial Recognition technology can bring to law enforcement;
- Explains the legal basis and wider framework and policies under which the Met can operate Live Facial Recognition;
- Recommends the consideration of a broad code of practice to guide the use of new and emerging technologies by policing.

How does the Met use Live Facial Recognition technology?

1. Live Facial Recognition is an operational tactic that helps the Met locate dangerous people who are wanted for serious criminal offences. It helps keep Londoners safe. We have published our legal mandate, policy and operating procedures for the use of this technology online[1]. Live Facial Recognition helps us spot those posing a risk of harm by monitoring facial images of people within a zone of recognition. Images from specially located cameras are searched against a watchlist of images of people who are wanted, or based on intelligence

[1] See https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition/ where the latest documents will continue to be published.

are suspected of posing a risk of harm to themselves or others. Where the Live Facial Recognition system identifies a potential match, the system flags an alert to an officer who considers that alert and makes a decision on whether any further action is required. If there is no alert, the biometric data is immediately and permanently deleted.

What benefits can Live Facial Recognition technology bring to policing?

2. Live Facial Recognition augments what an officer can do; it does not replace an officer. In fact, the Data Protection Act 2018 requires that automated decisions that affect individuals must have a human in the loop to oversee the decisions and processes behind them.

3. Live Facial Recognition can bring real benefits to policing, for example:

Knife and gun crime: Live Facial Recognition can assist the Met in fighting knife and gun crime. LIVE FACIAL RECOGNITION could be deployed to identify wanted offenders who have failed to attend court and the court has now issued a warrant for their arrest. Used in this way, LIVE FACIAL RECOGNITION would assist in the prevention, investigation, detection or prosecution of criminal offences.

Child sexual abuse and exploitation: Live Facial Recognition can assist the Met in fighting child sexual abuse and exploitation. Live Facial Recognition could be deployed based on intelligence to find vulnerable individuals who are missing and believed to be at risk of sexual abuse. Child sexual abuse investigations use significant police resources where the need to locate and make an identification is often time critical.

Terrorism: Live Facial Recognition can assist the Met in fighting terrorism. By way of example, Live Facial Recognition could be deployed at international borders. This could be part of tailored security measures to keep people safe. Live Facial Recognition can act as a valuable tool to assist officers to identify those of interest for terrorism reasons, including those who may be travelling on false documentation. Live Facial Recognition therefore supports officers who have the challenge of being familiar with a potentially significant and rapidly changing number of persons who are often motivated not to be identified and where the consequences of a missed identification opportunity could be catastrophic.

Missing and vulnerable people: At times, the police may turn to the public to help with identifying missing people by making public appeals. Typically, this involves circulating a photograph of a vulnerable person across the media. This action is highly intrusive to the individual's privacy rights given the aim of the public appeal is for wide-scale awareness and that information goes outside of police control when it is placed in the public domain. Where it might be viable to use Live Facial Recognition as a tool for identification instead, the intrusion on the individual's privacy rights can be lower, yet it still offers the Met a route to discharge its common law responsibilities to protect life.

Legal Framework

4. When policing uses technology such as Live Facial Recognition, it does so to meet a defined policing purpose, which must justify any privacy intrusion. The technology's effectiveness and demographic performance must be assured as fit for its intended purpose, its use must be transparent to the degree possible within a policing context, and there must be safeguards, supported by community engagement and suitable oversight.

5. Policing common law powers provide the legal basis for law enforcement to use Live Facial Recognition, as the 'Bridges' judgment confirms. Further regulation consists of a set of safeguards including those provided by the Human Rights Act 1998, the Data Protection Act 2018, the Equality Act 2010 and the Protection of Freedoms Act 2012. Under these sit codes and guidance from the ICO and the Surveillance Camera Commissioner, and our own policies and operating procedures. In addition to the strong legal basis, there is oversight from the Mayor's Office for Policing and Crime and various commissioners including those responsible for information, investigatory powers, surveillance cameras and biometrics.

A code of practice for technology

6. The Met recognises that there is a need for the use of technology to be both accessible and foreseeable to the public. It needs to be possible to work out how the technology is used, the rules which regulate that use and predict how they apply to the public. It is for these reasons that the Met believes it would benefit from a tech-agnostic code of practice to provide guiding principles for the introduction of new technologies, such as the Live Facial Recognitions of the future. In addition, a new code could provide a framework for ethical decision making; provide guiding principles to help forces be transparent and help the police engage with industry, partners and the community.

7. Technology has a critical role to play in fighting crime and keeping Londoners safe. Indeed, how could we justify to victims of crime that there is a technology out there that we did not use, a technology already routinely used in shops and bars, hotels and restaurants. Of course, when policing does use it, we must ensure we do so lawfully and proportionately. A code of practice would sit alongside College of Policing Authorised Professional Practice and individual force policy. It would ensure that the public understands how policing can consider and implement new and emerging technologies such as Live Facial Recognition.

Dr Peter Wagget, BSI Chair, IST/44 Biometrics Committee

IST-44 is a BSI group that develops biometric standards around biometric systems and their operations. It represents the UK and its interests at the European Committee of Standardisation. It represents the UK's interest at the International Organisation for Standardization. Our members comprise experts from industry, academia, government, and special interest groups. These experts have a large amount of understanding of the practical implementation and operation of biometric systems and an understanding of the underlying biometric recognition technologies including AI. These experts provide their advice on a voluntary basis.

Through the work with ISO we developed a range of standards that cover biometric data capture, biometric data interfaces, system operation, and biometric data storage. These standards are internationally recognised and are needed to support the use of systems that cover for example passports, driving licences, and provide seamless identification internationally. The information contained in these standards is necessarily very detailed and requires background knowledge to ensure it is interpreted correctly and meets the purpose of standards which is to develop systems that are safe, secure, widely accepted and understood, and transferable.

Public acceptance of these technologies has increased over time through widescale deployment of devices such as smartphones and tablets and all those devices that use such technologies. The number of organisations using such technologies have also increased over time. If you go back in time to 2011, we recognised this trend and produced a UK code of practice for the implementation of biometric systems. The production of this was sponsored and supported by the home office and the purpose was to provide a short reference document for established implementers, but also a clear starting point for any new users of biometric

technologies. It was intended to be easy to understand and provide a clear road map for new implementations to the wider standards landscape, to provide a checklist of activities to ensure they complied with existing rules and regulation and be as jargon free as possible. The development of biometric systems since 2011, using new technologies such as AI, and also the wide scale use of technologies across a range of different users, is pointing us toward the same situation we had at that time; which is that we need to go around that activity and revise and take account of the new technologies and the new use cases. My point is that we should look at something like Pass 92 and respectfully request support from the parliamentary group to revise it to include these new technologies.

Pauline Norstrom, Honorary Member, British Security Industry Association (BSIA)

Purpose and scope

The purpose of this document is to provide a positioning statement containing the British Security Industry Association (BSIA) evidence for the Evidence Meeting of the All-Party Parliamentary Group on AI to be held 11th October 2021. The BSIA position has been formed following discussion, collaboration shared experience of deployments and consensus of the membership.

Introduction

Thank you for inviting me to present to this session, I'm Pauline Norstrom, I am from a commercial background in video surveillance technology and now run an AI innovation advisory company. I am representing the BSIA as one of its honorary members. I have worked with the Association for over 20 years and during that time led a number of technology and ethics initiatives. Members cover all aspects of the private and national security process. These range from the development of specialised predictive AIs to front-line security officer services. Technology and services are integrated with law enforcement missions through public-private partnerships. BSIA is a stakeholder in the ethical and legal use of live facial recognition technology. Today I bring their ethical and legal guide as evidence of a way of doing things which explains why it is used, underlying ethics and laws and recommendations which should build transparency and trust.

How can AI technologies contribute to measures taken to ensure national security?

The private security industry customers are UK and global organisations from government departments, retail, education to smart cities. It ensures the safety of more than 70% of the population within publicly accessible places. Every sector has a security risk of some kind which is assessed, defined then mitigated through the maximum use of detection, communications and AI technology combined with the best quality trained people. It is a fact that most publicly accessible spaces are protected by privately owned cameras. Generally, it is the surveillance camera which captures images used in facial recognition systems whether that is through an AI built into the camera, or the images are analysed in the cloud. Many cameras deployed for general surveillance already have Live Facial Recognition capability although it is not switched on.

What are the potential dangers of using data-driven technologies in national security?

The private sector forms such a large component of the national security asset the Association became concerned about a potential ban resulting from irresponsible use by the authorities. The private sector already deploys facial recognition to verify access to establishments and services. It also came into its own during the pandemic when contactless technology helped to reduce virus transmission. In early 2020, a group of specialists was formed which embarked on the creation a guide which ensures uniformity and consistency. This included inputs of the members who develop and deploy the technology, analysis of the current legislation and consultation with key stakeholders in government.

How should regulation for a purposeful and safe deployment of Live Facial Recognition look?

We set out to clarify how it works and how it can be used. The ethical start point was the OECD's values-based principles for the responsible stewardship of trustworthy AI. These principles underpin the guide. There is no single clear piece of legislation in place to regulate the use of Live Facial Recognition in publicly accessible places. So we refer to the current laws which cover processing of facial special category data, camera images and their use by public authorities; such as UK GDPR, the Protection of Freedoms Act, RIPA, and the Equality Act. Also the range of regulators and oversight bodies from the ICO to the Biometrics and Surveillance Camera Commissioner and their respective voluntary guidance and opinion documents. There is a very clear differentiation between "one to one" verification to determine "is it you" and for "one to many" identification to determine "who is it". In the case of identification, we require that a human is in the loop and makes the final decision regardless of whether the technology is used for law enforcement or not. We saw this as a critical element of building trust in the use of the system and a means of improving quality through the reporting of any bias to the Live Facial Recognition developer. The guide also advises that there are standards already in place which define technical biometrics performance.

How should UK regulation compare to the planned risk-based EU law on AI technologies?

BSIA released the guide prior to the draft EU AI legislation and is supportive of the new EU framework.

How can the regular auditing of Live Facial Recognition technologies be guaranteed?

If there is risk-based classification and certification, we believe that auditing of Live Facial Recognition technologies can be guaranteed through post market monitoring. So if performance reduces due to learning from the environment the Live Facial Recognition must be withdrawn, corrected and re-certified.

How would individuals and communities be affected by the widespread use of Live Facial Recognition?

Currently, the public should be reassured that the lion's share of the video surveillance cameras are not owned and operated by the UK Government. And, unlike DNA, because there is no national surveillance camera or facial recognition database it is not currently possible to implement the widespread use of Live Facial Recognition. However, if it is used, individuals and communities should be reassured that they are safer in public places and only if they can make informed decisions about consent.

Concluding remarks

Concluding, the BSIA would like to see separate legislation for the use of surveillance cameras and Live Facial Recognition which aligns with the proposed EU regulation for high-risk AI. Also closer public-private partnerships supported at government level combined with a joined-up approach to informing the public where the high-risk areas are. As a result, transparency around when and why additional overt surveillance technology may be needed in these areas and how it is being used.

Lucy Holmes, Managing Director, Omni Telemetry and Associate Partner, 87 Holdings Ltd.

Omni's main purpose is to use data to drive labour and energy efficiency within buildings to optimise performance and reduce wastage. Within this space the question of live facial recognition is particularly interesting as most of the buildings we work with are very concerned about who is able to access their building or parts of their building which often contain highly sensitive and confidential information. However they are also concerned that those people that are allowed to access the information are then not subject to lots of surveillance due to the fear that this surveillance has the potential to be leaked or get in the wrong hands. One example I had recently was with a customer who had asked us to measure occupancy and air quality, however the technology had to be out of sight as there was a fear that this unknown technology would arouse unnecessary suspicion from valued customers who would use the meeting rooms to have highly confidential conversations. They were even concerned about the facial recognition technology which would unlock screens in the meeting rooms and these had to be switched off more often than not.

Although this is one example, I think this can be applied to the context of National Security as there seems to be somewhat of a dichotomy going on and a level that people are comfortable with that seems to have a very solid line that once crossed descends very quickly into mistrust, suspicion and dare I say it….fear. Arguably the very emotions that measures like Live Facial Recognition are attempting to eradicate.

The UK courts have concluded that "like fingerprints and DNA [a facial biometric template] is information of an "intrinsically private" character." The majority of us, I imagine, would not be super happy if before we entered a building or a shopping outlet or walked down the street we had to submit a sample of our DNA but at least in this instance and much like marketing

preferences we would have the chance to opt in or opt out of this and if we deemed that the risk of having our DNA captured, however quickly we were told it would be deleted outweighed the benefit of being able to walk down that street we could choose not to do it. Now this is an extreme analogy but it serves to illustrate the point that unlike this representation, in the case of Live Facial Recognition on a mass scale we rarely have this choice. We cannot easily opt in or opt out of having this 'intrinsically private character' captured.

This apparent lack of transparency I think is intrinsic to feelings of mistrust around Live facial recognition and despite the majority of us not being a threat to national security as we go about our day to day business I can't help but think that for a technology to truly realise its benefits building public trust and confidence is key.

We only need to go back to the A Level algorithm fiasco to highlight this point. A new technology, or certainly a new application of a technology that did not engender public trust, was not completely transparent and therefore was arguably bound to fail in its usage. Now I am left with the residual feeling that if the algorithm had given all the students their expected or higher than expected grades would we have had the level of outcry we did but nonetheless you've got to think that in the context of live facial recognition being used for national security where the implications are potentially considerably greater the potential ramifications of even the slightest whiff of gender, race, political or any other bias would be severe.

Do I think that live facial recognition could contribute to measures taken to ensure National Security, yes absolutely, but as Lindsey mentioned in her speech about the public needing to know how this technology is used and how it applies to them I do not think the bar has been met yet in terms of engendering public trust and confidence. And I do support the recommendation for transparency to begin to work towards this. However my recommendation would also be to really accentuate and bring to the fore all the good news stories that come with AI technologies for example in the medical space with surgeon less surgeries and early diagnoses. Make it clear that this is AI technology. Get AI more in the public space and get the public more comfortable with its usage and benefits and then perhaps the use of live facial recognition on a widespread scale can be revisited and we can truly realise its benefits.

To fully realise the benefits of Live Facial Recognition we need public trust and to engender public trust we need regulation to make use, application and the benefits of Live Facial Recognition transparent to the public, give AI a PR overhaul and bring to the fore good news stories, change the default dialogue which tends to favour negativity and suspicion and fully realise the benefits.

John Buyers, Head of Commercial, Osborne Clarke

What we will attempt to do is give a slightly different perspective on the use of Automated Facial Recognition (and Live Facial Recognition) to that provided by the other speakers. As many of you will be aware Osborne Clarke advise a number of private sector clients on the use and licensing of Automated Facial Recognition technologies.

In the context of the regulation of Automated Facial Recognition and Live Facial Recognition it is tempting to focus solely on the state sponsored surveillance use cases of this technology – after all they provide the most eye catching headlines. We mustn't ignore the way in which these technologies are also permeating products and services provided by private sector corporations. Examples include: Automated Building Access Control; Device unlock (such as on Apple's iPhone); Cashless Automated Facial Recognition enabled Retail – walk into a store, grab an item and leave; and Smart Advertising - used to target particular audience demographics.

Whether we want these targeted services and products is another matter but having advised businesses that are keen to launch in the UK and European market, I can say with confidence that the UK regulatory position is horrendously complicated and filled with overlapping regulation. There are three particular questions we typically ask when clients ask us to advise on this technology:

- Is your use of Facial Recognition for video surveillance (ie with CCTV)?
- Is it directly or indirectly State sponsored (ie use by the police, government agencies)?
- Is it being used on private property or in a public place?

Answers to each of these questions open up a raft of secondary questions – but the simple point to take away is that the regulation of state sponsored Automated Facial Recognition is completely different to private use.

There are nine separate statute laws, an international convention, and a code of conduct that could apply (depending on the answers to those questions), including the UK GDPR, the Data Protection Act 2018, The Protection of Freedoms Act 2012, the Police and Criminal Evidence Act 1998, the Regulation of Investigatory Powers Act 2000, the Intelligence Services Act 1994 the Police Act 1997 and the Private Security Act 2001. These are in addition to the Human Rights Act 1998, Article 8 of the European Convention on Human Rights and the Surveillance Camera Code of Conduct.

Notwithstanding these laws, there are five separate regulators that could potentially have jurisdiction over your use of Live Facial Recognition/Automated Facial Recognition: IPCO – The Investigatory Powers Commissioners Office; ICO – the In-formation Commissioner's Office; FSR - the Forensic Science Regulator; the Surveillance Camera Commissioner and the Office of the Biometrics Commissioner.

Oliver Dowden's recently launched a DCMS consultation led review into the role of Data in UK society (which is proposing the merger of the Surveillance Camera Commissioner and Biometrics Commissioner into the ICO for the purposes of police use of biometrics and surveillance) somewhat over-looks the fact that regulation is in fact bifurcated into private use as well as state sponsored use. In fact the private and commercial use of Automated Facial Recognition raises similar ethical concerns in relation to human rights and privacy, and rightly must be regulated. However, when used properly, it can be a significant aid to convenience and security. The National Strategy for AI does not cover this topic at all.

The reality of this fragmented approach in the UK is now acting as a disincentive to new entrants to the market – or at the very least putting them into a position where it is very likely that they are breaking the law (or at least in danger of doing so). To give a very real example, our personal and direct experience of advising clients in this area has made it evident that it is very difficult to legitimately launch a Cashless Automated Facial RecognitioN based retail solution in the UK.

Our advice has caused one major technology provider to "pause" the rollout of such solution due to regulatory concerns. There is another major market entrant and innovator that has opened cashless Automated Facial Recognition based grocery stores in the UK (replicating its USA model). It is clear that these stores are open in this country more due to an aggressive view from that particular company in relation to risk assumption (coupled with very deep pockets) than a desire to remain compliant with the prevailing framework – and can they be blamed when faced with this legislative muddle?

In our view, now is the time to take a streamlined approach which will provide consistent guidance for both the private users of this technology, and those that are sponsored by the state.

Contact

APPG AI Secretariat

Big Innovation Centre
14-16 Dowgate Hill
London EC4R 2SU
United Kingdom

info@biginnovationcentre.com
www.biginnovationcentre.com

appg@biginnovationcentre.com
https://uk.bicpavilion.com/about/appg-artificial-intelligence