White Paper

Corsight welcomes EU Commission proposals for a regulatory framework for development and deployment of artificial intelligence. This White Paper calls for;

- *Closer engagement from the EU with an industry that strives for compliance*
- *a clearer framework of standards to enable developers to show that compliance. The current framework requires strengthening*
- *Recognition that a 'human in the loop' development strategy is key to assuage public concerns over the use of this technology*
- *Organisational values and principles must irreversibly commit to only producing technology as a force for good*

Introduction

Regarding AI development it is clear that the EU intends to lead the world in setting the highest standards. Data protection, digital technology and the rights of the citizen are at the core of its thinking. The EU Commission proposes to harness development of artificial intelligence, machine learning and associated technology into a strong regulatory framework.

The proposals include establishment of an EU Artificial Intelligence Board, a comprehensive conformity assessment process, tougher fines for non-compliance and a newly refreshed Coordination Plan. These proposals are intended to generate increasing confidence in the use of such technology.

But what are the implications for the developer? Makers of software that will be classified as 'high risk' have taken great interest in these developments. Under the new rules all AI systems intended to be used for remote biometric identification of persons will be considered high-risk and subject to a third-party conformity assessment including documentation and human oversight requirements by design. High quality data sets and testing will help to make sure such systems are

accurate and there are no discriminatory impacts on the affected population.
These proposals must be welcomed. It must however be seen that facial recognition technology (FRT) is simply part of the whole surveillance system. The most important ingredient of which is the human at the centre of the process. Training, bias awareness, policies upon deployment, adherence to law, rules, regulations and ethics are key ingredients.
Developers must work with humans to create a product that is human intuitive and not the other way around. Consideration of providing legal and regulatory support in the use of such sophisticated software must be a foremost consideration for developers.
This White Paper sets out how organisations ought to develop their product in line with the new proposals and place the human at the centre of the operation.

Background

Our modern digital society is increasingly data driven and data dependent. As technology continues its relentless journey of evolution it is understandable that the challenges also increase.

In particular, artificial intelligence, machine learning and biometric related technologies are becoming increasingly sophisticated, increasingly prevalent and therefore increasingly intrusive to our lives. There are, arguably, few technologies which have commanded so much public comment in recent times than the use of facial recognition technology (FRT). With applications as diverse as unlocking your smart device, opening a bank account or controlling your passport entry to another country, the ability of FRT to be a tool which adds value to security and convenience in an increasingly populated world are more and more becoming an every-day fact of life.

Our growing population is both diverse and vulnerable in so many ways. In this digital age we must remain conscious of the precious rights and freedoms which we enjoy in a democratic society.

Whilst we increasingly rely more on technology, whether out of convenience or necessity, it is essential that we remain a free society, and an equal society which is devoid of the blight of discrimination. In the context of FRT it is one thing for the technology to conveniently open your smart device, it is entirely another for it to be used by a law enforcement

agency to seek you out for the purposes of arrest amongst a crowded place.

The Rule of Law

It is the law which provides the rules by which a society operates and which establishes the statutory safeguards by which our precious fundamental rights and freedoms are protected from illegitimate intrusion, whilst at the same time enabling institutions to act proportionately to keep us safe from harm.

In the context of new technologies, the challenge for lawmakers is to keep up with, and get ahead of, the evolutionary pace of development so that people can have trust and confidence in the actions of those institutions and the technologies they use in the public interest. Those challenges become particularly unsettling where applicable laws are either unclear, outdated and thereby less relevant or provide disproportionate discretion to those who operate technologies. This is where the new regulations will start to impact and drive standards upwards.

In a recent case before the Court of Appeal in England and Wales *(R (Bridges) v Chief Constable South Yorkshire Police)* the court ruled that the use of live time facial recognition technology in public spaces was unlawful in the particular circumstances before it. The court did not however rule that the use of the technology was unlawful *per se* when set against the applicable legal framework in England and Wales, which in this case was the Data Protection Act 1998 (and the subsequent Data Protection Act 2018), Common Law, the Surveillance Camera Code of Practice (June 2013 issued pursuant of the Protection of Freedoms Act 2012) and the policies provided by the police themselves. It was the absence of clear safeguards to constrain police discretion when determining who should be placed upon a watch list and where the technology should be used, which largely contributed to the court ruling on the particular point of lawfulness in the specific circumstances before it.

The industry must have a detailed knowledge, understanding and experience of the statutory and regulatory landscape operating in those particular circumstances, and of course wider afield. We therefore welcome the recent declaration made by the European Union to establish a pan European Data Governance Act. It is our hope that this legislation will provide much needed global and statutory leadership in the establishment of clear rules and guidance by which the use of

technologies such as FRT can be more confidently designed, produced and operated in a manner which maintains trust in safer societies.

Standards

It is not just the laws which are unclear and overlapping. It is understandable that technology advances at the speed of light; there is a commercial imperative. One look at the available standards against which AI software developers may aspire to, it is clear the picture is uneven, even muddled. This too is understandable given the new and evolving technology but as the industry moves rapidly forward it must not be held back. There is a continued need for developers to engage with international standards organisations to design and develop applicable standards. Afterall, without such standards, what measures will the EU conformity assessment framework measure against?

A Force for Good

Developers must recognise the power, the societal benefits and also the risk potential within the technology we produce. We strongly believe that those of us who build machines which have an impact upon society carry a responsibility, indeed a moral and an ethical duty, to ensure that they are only used as a force for good and to the benefit of the society and communities which our technology may help to shape.

Organisational values and principles must irreversibly commit to only producing technology as a force for good. The philosophy must surely be that we put the preservation of internationally recognised standards of human rights, our respect for the rule of law, the security of democratic institutions and the safety of citizens at the heart of what we do.

We hear and understand the voices of concern which are often raised in the context of FRT in particular, primarily issues of accuracy, bias and legality. We also understand the legal and ethical obligations which are applicable to those who use it.

The message is clear from the EU Commission. We recognise that simply producing the best AI is nothing unless it is ethically produced and legitimately operated in accordance with relevant laws. The proposed applicability of the new EU data regime to producers and users of technology alike is welcome as a clear and consistent legal standard

which transcends all parties and stakeholders operating in a partnership or other business or operational relationship.

The establishment of an external and independent process of conformity assessment with the new data laws is one which the industry must welcome and acknowledge.

Accuracy

Developers are acutely aware of the broader concerns and risks which arise when designing and building prejudices in software. Great care needs to be taken in training systems to operate in a multitude of operational contexts and ensure that they can be deployed lawfully and ethically when using images to accurately recognise human faces fairly, and consistently, across all diasporas.

However flawless our technology is when it is designed and produced, it can of course be abused when operated by a dysfunctional or oppressive end user. FRT is a powerful surveillance technology. Where inadequately regulated in a democracy, such dysfunction is a short ride away from dystopia.

This White Paper encourages developers to work closely with its client base to understand the user requirement and the legitimacy of endeavour. It encourages them to work collaboratively where necessary to enable and support client compliance to statutory obligations and to build appropriate safeguards where vulnerabilities may arise.

Equality

Inclusion and diversity must be central to a developers' efforts to ensure that any potential for the technology to discriminate against people or harm their human rights is removed. Linked to this, companies need to develop policies that clearly stipulate they will not trade with customers who do not support and uphold internationally recognised standards of human rights.

In the aforementioned "*Bridge's case"* the court found that the police use of live time FRT was not in accordance with the provisions of the Equality Act 2010 in those specific circumstances. It was determined that they had not taken all reasonable steps to satisfy themselves that no risk of bias

existed in the FRT they had used. It was not suggested that any such bias existed in that technology but the police should have done more to satisfy themselves as to such matters.

Companies must recognise that sometimes clients may not always have the depth of understanding of biometric technologies to ask all the questions or take all the steps reasonable to satisfy their due diligence obligations. Explaining in relatively simple terms how technology works, how it is built and trained, how it arrives at a decision, how to recognise signs of risk and providing a pathway for clients to take those reasonable steps, are just some examples of how companies must act. This helps to ensure that the processing of biometric data is properly considered and assessed as part of the data protection impact assessment (DPIA) obligations which arise.

It is important for clients to understand the extent of the capabilities of the technology. It is equally important that they are properly prepared and competent to use it lawfully. FRT is after all a biometric surveillance aid which recognises a face as being a human face and provides a similarity score when it recognises a similarity between a facial image captured with one held on a list of images held within its data base. The technology does not establish individual ‘identity’ – that is the job of humans. How those humans use the technology, how they make decisions and the actions they take when considering indications provided by algorithms are influenced by the competency and training of the individuals and the strategic and operational structures they work within.

Conclusion

Corsight AI anticipates that whatever the final iteration of new EU Data Protection proposals it must act as a profound force for good. It must provide further challenges and safeguards which guide the use of biometric surveillance capabilities towards a safer and more confident society.

We are clear that if the optimum outcome is to be achieved following any introduction of new regulations, it is imperative that the EU Commission continue to work with the industry, data scientists and practitioners.

In turn developers will need to embed privacy, ethics and data security more rigorously right across their organisations. Senior leaders will need to champion the philosophy of the new proposals to ensure future compliance if they are to survive.

This is a pathway along which Corsight has already proudly taken many steps along.

Tony Porter OBE QPM LLB

Chief Privacy Officer

Corsight Ai