What now for police and AI?

It is clear that the EU Commission intends to continue proactively upholding the rights of the citizen in its regulation of data and digital technology, which is a positive step in the right direction. Last month's proposals outline its plan to harness the development of artificial intelligence (AI), machine learning and associated technology into a strong regulatory framework. 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. This will be policed in a similar manner to the EU's data privacy legislation, GDPR, which gives the EU the ability to fine organisations that infringe its rules up to six per cent of their global turnover.

However, although there are exceptions to this prohibition, including allowing police forces to use facial recognition technology (FRT) to find the 'suspects' of any serious case that carries a minimum three-year sentence, the approach taken by the Commission risks creating a regulatory patchwork, as some authorities may choose to limit or withdraw the use of facial recognition in police operations.

The EU AI Trustworthy Assessment Framework, released in 2020, informs many of the proposals and provides a more considered and ethical approach to the legitimate use of FRT. Police often have no choice but to leverage facial recognition and other technologies to keep people safe.

This is the direction that best serves the public interest as opposed to a knee-jerk call to ban a tool that has proven public safety benefits; namely protecting the vulnerable and targeting the most serious and organised criminals. In an increasingly complex world, crime and terrorism operate across borders, both nationally and internationally. Instances of child trafficking, sexual exploitation, drug trafficking are expanding between nations and this technology provides a tool in the armoury of our protective agencies.

We cannot deny FRT needs to be deployed and utilised ethically and legitimately and we support the views expressed in the recent Court of Appeal case in June 2020 (Bridges v South Wales Police). However, we must allow our overstretched and under-resourced law enforcement agencies to fight crime without one hand tied behind their backs. We certainly believe greater clarification on policy, oversight and guidance is required. This must include a stronger partnership between government and software developers.

The latter must always understand and act upon the importance of privacy and security in the design, implementation and operations of AI systems. Governments must continue to introduce more effective legislation and regulation; it would be a promising progression if a new regulatory body streamlines guidance and provides a better framework for organisations. Without a doubt we want to prevent AI abuse. But this cannot mean banning facial recognition altogether. The police are calling for clearer and more consistent guidelines and it is time that the Government fulfils its commitment in the 2019 Manifesto and delivers upon that promise.

The public distrust of this technology typically derives from misinformation or ignorance as to how and why FRT is used. Moreover, what critics fail to recognise is that biometric surveillance is based wholly on a 'human in the loop' strategy and should always be dependent on human intervention. While the software provides the likelihood of a match, the accompanying policies and processes are aimed at ensuring an operator can conduct the surveillance lawfully. Strategic governance overlaid by an organisation is equally as important. It enables transparency, accountability, confidence and integrity. The EU must, therefore, factor this into its legal framework when discussing the application of FRT – as AI FRT systems are always subject to human control. An expansive and embracing approach is required. This technology can and must be seen as a force for good.

Tony Porter
Chief Privacy Officer at Corsight AI and former Surveillance Camera Commissioner.

High-risk stakes for AI – see p24

POLICEPROFESSIONAL

is published by
Modus Media
117 The Midlands
Holt
Trowbridge
BA14 6RJ
Tel: 0333 320 8004
ISSN 2041-8809

Managing Editors
Paul Jacques
paulj@policeprofessional.com

Tony Thompson
tony@policeprofessional.com
@PolicePEditor

Contributors
Paul Jacques, Tony Thompson, Professor John Coxhead, John Hicks, Richard Millett, Bernd Carsten Stahl, Sally Bibb, Richard Davis, Rebekah Tomlinson, Dan Millward, Julian Hayes, Andrew Watson, Tony Porter.

Editorial
Tel: 0333 320 8004

Advertising
Tel: 0333 320 8004

Subscriptions
subscriptions@policeprofessional.com

Yearly subscription rates

Print only	£137 UK £254 Europe £333 Rest of World
Online only	£136
Combined	£155 UK £269 Europe £348 Rest of World