Facial recognition: how policing in Scotland makes use of this technology

I refer to the above and thank you for inviting the Scottish Police Federation (SPF) to contribute to the work of the Committee.

As professional observers, police officers look at faces on a daily basis, compare them with images we have retained in our own memories and act upon them appropriately. It is a core function of being a police officer.

Facial recognition technologies can complement these skills and allow that activity to be undertaken on a much larger scale using that same reference data.

Applications

The SPF see many facial recognition applications that in future could assist with policing and public safety including;

- The ability to scan crowds and public spaces with cameras for missing children, vulnerable adults or wanted persons;
- The retrospective identification of individuals by comparing suspect images against a gallery of known criminals to assist us in identifying perpetrators many times faster than we could do manually;
- The future identification of individuals with whom Police Officers are interacting with (through bodycams) and in particular recognition of those predisposed to violence or who are vulnerable.

The Current Environment

Facial recognition is a technology we all encounter with increasing frequency. Whether it be at automated passport gates at airports, access to electronic devices or within digital photographic applications. The public appear comfortable with its application and with a steady stream of fictional TV films and dramas they have an expectation that Policing already has a capability far beyond reality. The truth is that the image processing capabilities accessible through a single smartphone currently exceeds that of most UK police forces.
We would also suggest that as an industry expected to be worth $7 billion by 2024 in the US alone\(^1\), it is a technology that is here to stay.

**Sharing of data**

The consultation specifically references the sharing of data for facial searches on the UK PND system. The practice of police officers sharing images of criminals with officers in other Forces is fundamental to collaborative policing and the recent successes of PRÜM (sharing of DNA data) across Europe underpins that.

In principle then the comparison of facial data with data held on Police National Database is no different and should be seen as a positive step forward. If we don’t use such automation then the task would require to be carried out manually if at all.

**Acting on Matches**

Facial identification has much in common with Automatic Number Plate Recognition Systems (ANPR) in that neither is fool proof. Masks, headwear and even makeup can be used as disguises to fool systems. Like ANPR, we believe a match should be considered as intelligence and human verification must always take place before acting upon it. This is a principle that Police officers are comfortable and familiar with.

**Governance**

There have been a number of applications of facial recognition in commercial environments that have raised concerns. Most of these however relate to the management, use and retention of private data, not to the technology itself.

Police Scotland however, operates in a different environment. It has access to a rich dataset of legally held images from criminal record and intelligence systems.

SPF sees no difficulty in comparing the results of a facial algorithm taken from a camera with the results of photographs held in our own systems, as long as agreed rules of proportionality, necessity and retention are adhered to. In many cases these will be more stringent than those under which Police Officers work under eg. Police Officers can’t be made to forget who they have seen.

Our view seems to chime with research from the Ada Lovelace institute\(^2\) that shows the 70% of the public support this technology in Police Criminal investigations.

SPF would therefore urge a proportionate response in relation to the governance of facial recognition technology. The creation of a Biometrics Commissioner should provide a good independent review authority to establish codes of practice and oversight but fundamentally this is an issue about the use of police data and its use, for which there are already well established protocols; oversight laws and frameworks.

\(^1\) [https://www.marketsandmarkets.com/Market-Reports/facial-recognition-market-995.html](https://www.marketsandmarkets.com/Market-Reports/facial-recognition-market-995.html)

Governance of the Police use of this technology must also be considered in the context of other sectors. Almost all of us have had our faces processed by algorithms belonging to companies such as Google, Amazon and Facebook, with little complaint. Indeed many people now actively submit their data to these companies for the convenience of the benefit they get in return - a social network, photo indexing or even smartphone functionality.

Perhaps the most remarkable finding in the Ada Lovelace Institute survey is that the support for this technology to be used by Police in Criminal Investigations is 16% higher than that relating to that for smartphone access and 20% higher than its use at airports - both of which are currently in widespread use.

In a policing context, not only will facial recognition be more regulated and accountable but the benefit is a demonstrably more safe, more secure society for all.

**Funding and Partners**

The complexities of facial recognition technologies do require significant computing power and the advanced neural network technologies that can process images are expensive. Given the capital position that Police Scotland is currently in, any investment in this technology does however seem unlikely without partnering with 3rd party contractors. This of course has its vulnerabilities but if facial recognition is considered through the prism of data governance then this is familiar territory for law enforcement.

In conclusion, the SPF believes facial recognition technology offers an opportunity for Police Scotland to work more efficiently and effectively. It allows it to access technologies that the public would expect it to have access to. Some work will be needed to set out rules and codes within which the Service can operate but this must not be burdensome or overly bureaucratic.

We also urge that the police use of this technology be considered entirely separately to that of commercial operators and suggest a distinct programme of public education be undertaken to reassure the public what the technology is, and more importantly, isn't.

David Hamilton
Scottish Police Federation
1 November 2019