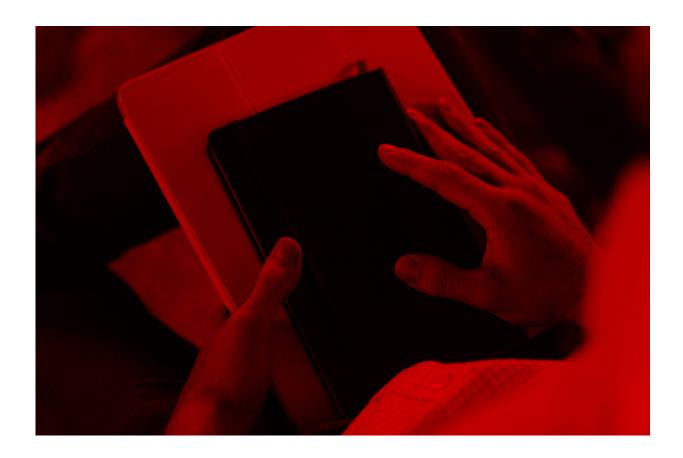# Relationship between big tech and policing is shielded behind commercial confidentiality

August 4 2021, by Katerina Hadjimatheou

Credit: Tima Miroshnichenko from Pexels

For over ten years, public inquiries, press reports, police whistleblowers—and even chief constables—have been raising the issue of police IT systems not being fit for purpose and ultimately failing

victims of crime. This has prompted significant media attention and public scrutiny, as well as the resignation of the head of one force.

But the role of the private technology companies behind these reportedly failing systems has not been closely examined. Just three big developers are being paid tens of millions of pounds to supply the majority of these UK systems—and it's time a light was shone on them too.

The market is dominated by the Japanese-owned tech giant NEC, a US-based specialist provider Niche RMS, and the UK-based Capita which supplies four forces. According to my ongoing research, at least 41 of the UK's 43 forces are now the proud owners of a commercially produced integrated data system. According to their own websites Niche serves 26 forces with NEC serving 16. My own research suggests that Capita is offering its services to about four forces.

Government directive

Large scale investment in new police data systems in the UK follows a government directive requiring police to improve the way they collect and share intelligence. This directive came following a 2004 public inquiry into the murders of schoolgirls Holly Wells and Jessica Chapman by a known sex offender in Soham, Cambridgeshire. The inquiry found that better police data practices could have prevented the crimes.

Since then, police forces across the UK have embarked on a massive procurement spree, buying complicated data systems, chiefly from these three large multinational technology developers.

As well as being paid huge sums to design and implement the systems, these companies are often granted long-term contracts to provide IT services and maintenance on an ongoing basis, fixing errors and glitches, developing new functionalities and redesigning parts that are not

working well. As these public-private partnerships become an ever-more embedded feature of UK policing, it is time to start asking whether they work in the public interest—because there have been examples which appear to call this into question.

In June, the new chief constable of Greater Manchester Police (GMP) admitted that his [force](link)'s £27 million crime reporting system "[doesn't work](link)" and may need to be scrapped.

> "There is a systemic issue of the under-recording of crime."
>
> Greater Manchester Police Chief Constable, Stephen Watson, comments on the force leaving 220 crimes a day unregistered, adding that GMP will reform systems to increase the recording of crime
> [#Newsnight](link) [pic.twitter.com/Tf0Cq0a7zn](link)
>
> — BBC Newsnight (@BBCNewsnight) [June 28, 2021](link)

iOPS

His admission follows a troubled year, in which the force was placed in "special measures" by inspectors, leading to the resignation of his predecessor following a [snap inspection](link) of the "iOPS" IT system developed by Capita which found that 800,000 crimes and 74% of child protection incidents had mistakenly gone unrecorded.

[Further reports](link) then emerged that "a dataset of personal information"—including the names and details of sexual assault victims—was made available online, leading to massive breaches of privacy, although blame for this has not as yet been attributed to a failing of the IT system.

Athena and Connect

But GMP is not the only force having serious problems with IT systems. In 2019, it was reported that the "Athena" platform, which cost £35 million and which enables data to be shared instantly across nine UK police forces, was "unfit for purpose." Frequent crashes of the system and overly complicated processes meant police were failing to charge criminals in time for cases to make it to court.

Similar issues were raised in 2015 when Essex police was reportedly forced to turn to pen and paper after the Athena system crashed for days. Developers Northgate Public Services—which have since been taken over by NEC—apologized at the time for problems "in small areas" which it said it was fixing. Northgate's Connect platform, which forms the basis for Athena, is in use by 16 forces.

Niche

And in 2009, West Yorkshire police acknowledged in response to a freedom of information request that their introduction of the new "Niche" platform had "led to wrongful arrests." However, they also said the "critical perspective of Niche" was a result of their efforts to "identify areas for improvement."

The problems appear to be widespread. A 2018 survey found that only 2% of police officers nationally were satisfied with their IT systems, and only 30% thought their force invested wisely in them.

Police data systems have received much less media attention than more captivating, futuristic technologies like facial recognition and predictive policing. But they have far greater implications for the way people are policed today.

They determine what data police can record, how they record it and how easily that data can be accessed, shared, analyzed and corrected. When the systems glitch, crimes are left un-investigated, victims are failed, innocent people are arrested and criminals escape justice—as the cases of Manchester, Essex and West Yorkshire have already shown.

And when the data they supply turns out to be incomplete, unreliable, or erroneous, facial recognition techniques will pick out the wrong faces and predictive policing will pick out the wrong people.

The relationship between big police tech and policing is shielded behind commercial confidentiality—it's time the government opened it up to proper public scrutiny.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation