THE POWER OF INFORMATION

HOW TO UNLOCK THE POTENTIAL OF DIGITAL, DATA AND TECHNOLOGY IN POLICING

RICK MUIR

OCTOBER 2024

THE POLICE FOUNDATION
The UK's policing think tank

THE POWER OF INFORMATION:

HOW TO UNLOCK THE POTENTIAL OF DIGITAL, DATA AND TECHNOLOGY IN POLICING

Rick Muir

About Virgin Media O2 Business

We partner with over 550 public sector organisations across health, justice, local and central government, providing them with technology initiatives that build a positive work culture and deliver a superior experience for members of the public. With our expanded network, over 1,000 experts and engineers on hand and a former senior police officer as our dedicated Justice and Policing Lead, we work with over 30 UK police forces and other policing-relevant partners to develop solutions that outwit tech-savvy criminals and enable seamless remote working.
https://www.virginmediao2business.co.uk/public-sector/

About the Police Foundation

The Police Foundation is the only independent think tank focused exclusively on improving policing and developing knowledge and understanding of policing and crime reduction. Our mission is to generate evidence and develop ideas which deliver better policing and a safer society. We do this by producing trusted, impartial research and by working with the police and their partners to create change.

Steering group

Tony Blaker QPM, Chief of Staff, Digital, Data and Technology Coordination Committee, NPCC

Paul Court, Assistant Chief Constable, Sussex Police

Phil Davies, Temporary Assistant Chief Constable, Lancashire Police

Ian Dyson, former Commissioner of the City of London Police

Nick Gargan, policing technology consultant

Charlotte Hails, Head of Public Sector Vertical Strategy, Virgin Media O2 Business

Giles Herdale, policing technology consultant

Bethan Page-Jones, Head of the Capabilities Reform Unit, Home Office

Dr Rick Muir is Director of the Police Foundation

Cover: istockphoto

CONTENTS

GLOSSARY

BWV	Body worn video
CIO	Chief Information Officer
CSA	Chief Scientific Adviser
DDaT	Digital Data and Technology
ESMCP	Emergency Services Mobile Communications Programme
ESN	Emergency Services Network
IAM	Identity access management
NEP	National Enabling Programme
(N)LEDS	(National) Law Enforcement Data Service
NMC	National Management Centre
PDS	Police Digital Service
PNC	Police National Computer
PND	Police National Database

POLICE

1. INTRODUCTION: THE POWER OF INFORMATION

Policing is an information business. It is, at its heart, an exercise in managing risk using the information available to it. And yet so much of the information available to policing, that could be used to help keep people safe, is not being fully deployed because the police service is not realising the potential of digital, data and technology.

Too many police officers complain of having to enter the same data multiple times on different systems, of not having access to the right technology at work and of having to work with equipment that is much slower and more cumbersome than that which they use in their personal lives. Too much of the new technology that is purchased in policing is not fully utilised because of a lack of awareness and practical knowledge of how to make the most of it.

Too many police technology programmes have wasted vast sums of money while simultaneously failing to deliver the transformed service they promised. Too much police data, far from flowing through the system to enable intelligent decision-making, is locked away on local police servers, unable to be shared with colleagues in other parts of the country or with other public service professionals locally. Most public money invested in police technology is spent on maintaining existing and often outdated systems rather than on the new technologies that could transform the service in the future.

This paper is an attempt to address the question of how policing can make the most of digital, data and technology to keep the public safe and maintain the trust and confidence of communities.

The paper comes in three parts.

First, it assesses the current state of digital, data and technology in policing and how this enables, or indeed prevents, the effective use of the information the police hold to carry out their work.

Second, it identifies several major challenges that the police service must overcome if it is to realise the full potential of digital, data and technology.

Third, it makes recommendations to police leaders and policymakers that, if acted upon, could unlock the power of data, digital and technology in policing, which in turn should make the police more effective, efficient and legitimate.

The report also contains a number of case studies, both positive and negative, of police technology programmes and strategic initiatives, from which we derive some lessons.

This report is based on a review of the existing literature on UK police technology, including academic research, independent analyses of the various national policing IT programmes and current digital policing strategies. We also undertook 22 interviews with leading stakeholders including local Chief Information Officers (CIOs), national police leaders with strategic responsibilities, Home Office officials, the leaders of major national IT programmes and representatives from industry, both big and small.

The project was supported by a Steering Group which provided invaluable advice as to the key themes we explored, feedback on the recommendations and access to the many leaders we spoke to. The members of the Steering Group are listed on the inside front cover of the report and while the content and conclusions are the author's alone, the report would not have been possible without the Steering Group's generous time and support.

POLICE

2. THE CONDITION OF DIGITAL, DATA AND TECHNOLOGY IN UK POLICING

The history of policing has been driven in large part by technological innovation. In the 1930s Captain Athelstan Popkess of Nottinghamshire Police initiated trials in the use of radios to enable real time communication between officers on patrol and their colleagues at the station (BBC, 2009). He combined this with the use of police patrol cars, a combination which was to transform policing into its modern operational form.

In the early 20th century the Metropolitan Police first started using fingerprinting techniques to identify suspects and provide evidence to the courts, forensic techniques which remain critical to criminal investigations to this day (Critchley, 1978).

In the late 1980s police in Leicestershire managed to use DNA evidence for the first time to secure the conviction of Colin Pitchfork for the rape and murder of two teenage girls (Kilburn-Wilson, 2023). The rapid spread of CCTV cameras across the UK from the 1980s onwards created a new source of investigative data, to be followed by ANPR cameras that identify vehicle licence numbers and more recently cameras using facial recognition software to identify both suspects and victims.

In 1974 policing properly entered the computer age when the Police National Computer (PNC) went live, enabling police forces to access a database of lost and stolen vehicles. Over time the PNC would be augmented to include data on known criminals (with links to DNA and fingerprint data), vehicles, stolen and recovered property and driving licence data. The system still operates today and contains data on around 13 million people. However, the PNC is now so old that the Home Office cannot find companies with the expertise to maintain it (Davies 2021).

The precarious state of the PNC is in many ways symbolic of the wider state of police data and technology. While there have been some notable successes in recent years, such as the spread of Body Worn Video (BWV), the big story is the continued reliance on outdated technology rather than the use of data and technology to transform policing. The reasons for this failure will be explored in the next chapter, but here we review the current condition of digital, data, and technology in UK policing.

2.1 OUTDATED TECHNOLOGY

Much of the technology police officers and staff use at work is woefully outdated compared to the digital devices they use daily in their private lives. In a 2018 survey of almost 4,000 police officers in England and Wales *Policing Insight* found that:

- 55 per cent were not satisfied with their force's ICT provision.
- Just 30 per cent thought their force invested wisely in technology.
- Just 42 per cent thought the main systems in their force were easy to use.
- Just 18 per cent said their force's systems were well integrated.
- Only 50 per cent said the information on their force's systems could be relied upon.
- Just 65 per cent said they were able to access a computer at work when they needed one.
- Just 55 per cent said they could easily access support with ICT when they needed it.
- Only 27 per cent said that the ICT related training they received was of high quality and was provided at the right time.

(Policing Insight, 2019)[1]

[1] The fact that the most recent survey of the police workforce on the state of digital, data and technology is six years old is a concern. Undertaking a new survey should be a priority for future research.

In free text responses officers described problems such as:

- Server drop-outs and bandwidth issues.
- Systems that were not user friendly and which wasted time.
- Inadequate training.
- Broken printers, a lack of computers and screens that were too small.
- Duplicated data entry.
- Police systems that were incompatible with partner systems or other police systems.
- The continued use in some forces of handwritten statements.

(Policing Insight, 2019)

Although there have been improvements since 2018, such as the rollout of Microsoft 365 through the National Enabling Programme, there is little reason to think these basic issues of outdated technology do not continue six years on. Indeed, in her recent joint Police Foundation lecture with Sir Mark Rowley, Dame Lynne Owens, the Deputy Commissioner of the Metropolitan Police, said that,

> *'The lack of a strategic plan for policing means that improvement and collaboration in IT has been woefully slow. We risk slipping further and further behind the private sector through the loss of investment, precipitated by the loss of capital grants from government, and lack of join-up.'*

2.2 TECHNOLOGY DEBT

Rather like someone struggling to pay off a large loan, spending their money on higher interest payments and never reducing the principal, the police service is carrying a large amount of what a number of our interviewees described as *'technology debt'*. One of our private sector interviewees commented

> *"our analysis shows that 90 per cent of current police IT spend is going on maintaining legacy systems rather than investing in technology that will transform services."*

A number of stakeholders we spoke to commented that the police actually spend a lot of money on technology (£1.4 billion per annum) but because the vast bulk of this expenditure goes on, in one interviewee's words, '*keeping the lights on'* the public is not getting the value it should from that investment (NPCC/APCC 2020).

As one police technology leader told us

> *"most police IT strategies are replacement strategies"*

aimed at simply updating existing systems rather than thinking strategically about how technology can use data to radically improve the service it provides.

2.3 DATA CHALLENGES

The technology debt problem is compounded by significant data challenges. As one police leader told us,

> *"we need to attend to the basic issues of data quality, data standards and data sharing".*

There are two aspects of this that are worth pulling out. First, there is data that has been incorrectly entered with, for example, errors in the spelling of names and places, or with information entered in the wrong category. Barely half of respondents to the 2019 *Policing Insight* survey thought that the information on their force's systems was reliable.

Apart from the obvious problem of trying to make sense of erroneously inputted data, these data quality issues make it harder to share data and to use data as a training ground for Artificial Intelligence technologies such as machine learning tools. AI technologies learn from large data sets, but if those datasets are error strewn, then they will learn from biased and inaccurate information. As one police technology lead commented

> *"you put garbage in and you get garbage out".*

Interestingly we were told that alternative AI tools might be able to help cleanse the data and the drive to adopt AI tools might now be a driver for sorting out some of these data quality issues.

Second, there is a large volume of outdated data sitting on police servers. One interviewee told us that

> *"we are non-compliant with the ICO (Information Commissioner's Office), and have this massive collateral, we're storing it and it's costing us a fortune."*

This is a form of *'data debt'* that the police have never tackled, probably due to a desire not to lose any information they think might be useful in the future and also due to the complex legislative and regulatory requirements surrounding the management of police information.

In addition to these data challenges, there is the issue of data that has been inconsistently entered onto systems both within and between forces. It is to this question we now turn.

> ***"According to our interviewees, the lack of interoperability is probably the biggest single obstacle to policing being able to exploit the power of the data it holds."***

2.4 A LACK OF INTEROPERABILITY

One of the biggest problems with police technology is the lack of interoperability between the core systems run by the territorial forces and the various national agencies. Forces have invested in different Records Management Systems (normally either Niche or Athena), different contact management systems, different digital evidence systems and so on. They are locked into contracts with different suppliers, meaning that these systems will need replacing at different times. This makes it hard to achieve a coordinated approach to interoperability.

The daily impact of this is that officers have to enter the same information in different formats on different systems, must log in multiple times, have to undertake multiple searches for the same person or address on different systems, and struggle to share data with colleagues in other forces or professionals in partner agencies. According to our interviewees, the lack of interoperability is probably the biggest single obstacle to policing being able to exploit the power of the data it holds.

The lack of interoperability is a feature within local forces (where information about people, places and so on exists in multiple places in different formats), between local forces (where information has been collected inconsistently and is held within 'walled garden' systems), between the police and other organisations such as the Crown Prosecution Service and the courts, and between police forces in this country and those overseas.

At each of these different levels, data is not being shared that could make a critical difference to public safety. It should be recalled that it was in part a lack of data sharing between Humberside and Cambridgeshire Police that enabled Ian Huntley to murder Holly Wells and Jessica Chapman in 2002. In that case information relating to serious criminal allegations against Huntley held by Humberside Police was not in the possession of Cambridgeshire Police prior to Huntley applying for a job as a school caretaker. Nor was this information available to Cambridgeshire in the early weeks of their murder investigation, in which Huntley was thought to have been the last person to have seen Holly and Jessica alive. Interoperability sounds like a dry technical matter, but in policing improving information sharing could unquestionably save lives.

> ***"Although not unique to policing it is notable how many major national police IT programmes have overrun, cost way more than planned and failed to achieve their original objectives."***

2.5 THE FAILURE OF MAJOR NATIONAL IT PROGRAMMES

Although not unique to policing it is notable how many major national police IT programmes have overrun, cost way more than planned and failed to achieve their original objectives. Take, for example, the replacement of the Airwave network which enables secure radio communication between the emergency services. This project started in 2015 and remains incomplete almost a decade later, with the police, ambulance and fire services still using Airwave, despite the government spending £2 billion on the development of an alternative system (see Case Study A).

Or take the National Law Enforcement Data Service (NLEDS) programme which was launched in 2016 to replace the ageing PNC and merge it with the Police National Database (PND), which holds intelligence data. PNC has still not been replaced, despite no companies being able to maintain it beyond the end of 2024. The government has now given up on the idea of merging PNC with PND and the programme has cost 68 per cent more than originally planned (see Case Study B).

In the case studies below, we highlight some of the lessons to be learned from these national police IT programmes.

Case Study A. The Emergency Services Network

The Emergency Services Network (ESN) was proposed in 2015 to replace the existing Airwave network. 108 police, fire and ambulance services across England, Scotland and Wales were to use the network to enable communication between the field and control rooms. The Home Office's intention with the ESMCP (Emergency Services Mobile Communications Programme) was for it to be a more cost-effective alternative, while providing those who used the network with current mobile data.

As David Hillard notes,

> *"Cabinet Office Minister Francis Maude spotted an opportunity to cut costs by renegotiating the contract with Airwave, the existing emergency services communications network owned by the Macquarie Group. Macquarie refused to play ball, so, in 2011, the government decided to 'act tough' and announced it would replace Airwave with a brand-new system called ESN… The government claimed that Airwave's TETRA technology was becoming obsolete and the emergency services would benefit from improved communications, including video and data, at lower cost if they utilised the UK's new commercial 4G network capability. This was a blatantly a politically motivated decision that no one wanted, especially the emergency services."* (Hillard, 2023).

As one of our interviewees told us, a key lesson here is

> *"do not force a solution on the users."*

In 2015, the Home Office signed two separate contracts to deliver this programme: one with EE to provide priority access to its mobile network and to increase network coverage and another with Motorola to develop the software and systems (Davies, 2023).

As early as 2016 the National Audit Office (NAO) determined that the programme was high risk because of the commercial approach taken, the ambitious expectations of what was technologically possible within the time frame and concerns that the users would not accept the new system (Davies, 2023). Notably in 2016 Motorola purchased the existing Airwave system, which created a conflict because they were then both making money from keeping the old system going while being contracted to develop the new system.

In 2021 the Home Office recognised this risk and determined the profits Motorola was making from Airwave were

> *"excessive and disincentivised it from completing its ESN contract".*

The government said it would force Motorola to sell Airwave, but instead Motorola indicated it would rather withdraw from the ESN programme. The ESN contract with Motorola was ended in 2022, with no alternative system for Airwave in place. The Home Office did not receive the systems and software necessary to deliver the ESN and will not use Motorola's work when ESN is live (Davies, 2023).

The Home Office estimates that between April 2015 and March 2023 it spent £2 billion on ESN and another £2 billion on running the existing Airwave network. In 2018 the deadline for turning Airwave off was extended until 2022 and then in 2021 it was again extended to 2026 (Davies, 2023, p.6).

The NAO notes that while Airwave cannot last indefinitely it could last well into the 2030s and there is still a concern that the new ESN technology will not work at scale across the new network (Davies, 2023). As Hillard notes:

> *"crucially, 4G/5G technology still cannot deliver 'device-to-device' communication that enables frontline emergency service workers to talk to each other in life-and-death emergencies when the wider network is unreachable in rural locations or deep inside buildings."*

As one of our interviewees told us,

> *"they were forcing the technology to bend to the policy and the finance."*

The Emergency Services Mobile Communications Programme is now taking a more modular approach to adoption.

Case Study B. The Law Enforcement Data Service (LEDS)

The Home Office manages two major police information and communication systems; the Police National Computer (PNC) and the Police National Database (PND).

PNC has been the main database for criminal records since 1974, used by officers from all 45 police forces in the UK, alongside 127 other organisations which need access to the data. PND was introduced in 2011 following the 2004 Bichard Inquiry into the Soham murders, which found that a lack of information sharing between police forces was partly to blame and recommended that a national police intelligence database be created.

The Law Enforcement Data Service (LEDS) was launched in 2016 to take over from the PNC and PND, which "are reaching the end of their useful lives" (Davies, 2021) resulting in a joined-up approach where the data and systems can be linked. Since then, there have been issues with costs and further delays and contracts for the PNC and PND have been extended.

According to the National Audit Office:

- By 2021 the programme was already overdue, had not delivered the expected services and the total costs had increased by 68 per cent to £1.1 billion.
- The Home Office has had to concede that it is not possible to merge the two systems within the time frame and it will now focus on replacing PNC alone.
- An external programme review commissioned by the Home Office in 2020 found that the causes of the delay included uncertainty around the scope of the requirements, de-prioritisation of funding relative to other programmes, changes in technical approach, a lack of commercial strategy and shortcomings in programme management and governance.
- The Home Office and the police have not had a consistent shared understanding of the intended outcomes of the LEDS programme. One of the lessons, as one of our interviewees told us, is that

> *"the users of the technology need to be fully involved in the process."*

- The increasingly fragile PNC system has not been replaced, bringing greater risks for police operations and requiring the police to bear more cost.

> *"The Department cannot yet guarantee to the police that a replacement system will be in place in December 2024, when the PNC's current technology will no longer be supported." (Davies, 2021, p.9)*

Case Study C. The National Enabling Programme

The National Enabling Programme (NEP) was launched in 2020 to introduce commercial cloud computing to UK forces. It included three strands:

- Identity Access Management (IAM): to provide a nationally-supported identity solution for police across England and Wales. It is designed to help forces manage access to devices used by officers and staff.
- National Management Centre (NMC): a central cyber-security unit to monitor forces' on-premise and cloud-stored information.
- Productivity Services: exploitation of the Microsoft 365 application suite and Azure Information Protection security tools. Critically this included access to Teams that became business critical during the pandemic.

The programme has been widely considered as a success, winning awards including 'Security Project of the Year 2020' at Computing's Digital Technology Leaders Awards 2020, and also the award for 'Risk Management' (as well as being shortlisted in the 'IAM Award' and the 'Special Award: Pandemic Resilience') at the Security Excellence Awards 2020.

Interviewees highlighted the following factors as key to the successful roll out of the NEP:

- It took a modular approach, allowing forces to take up different aspects when they were ready to do so.
- It was police run and designed around operational requirements.
- It made use of existing reliable off the shelf technology such as Microsoft 365.
- It took place during the Covid 19 pandemic which focused local chiefs on the need to improve their ways of working to respond to the crisis.

However, a number of interviewees felt the programme had ended prematurely and before the full benefits could be realised. Some considered that with a little extra funding much more could have been done to maximise the potential of the new capabilities introduced.

Case study D. Single Online Home

Single Online Home (SOH) is a programme to provide nationally consistent, locally branded services, brought together in a single 'digital police station'. It was launched in 2018. The NPCC vision for the programme was that

> *"the experience of connecting with police through digital channels will be as helpful, personal and reassuring as approaching an officer on the street".*

SOH allows the public to report crime, request information, submit firearms licence applications and much more, with around 40 different policing services available online. All but two police forces have now adopted SOH.

According to those leading the programme, key enablers for it's success have been:

- The fact that it was rolled out gradually and voluntarily, with adoption resting on a persuasive business case;
- The use of pathfinders which meant that those forces that were keen to go first and test it could do so, without being held back by others who were not ready for adoption;
- The flexibility of the programme, whereby forces can choose to make use of varying degrees of functionality;
- The fact that the capital costs of the programme have been paid for centrally, which, along with the fact that it offers improved services, has compensated for the fact there are higher revenue costs than the status quo;
- The way technology has helped to manage the data effectively, which means the system has been able to deal with the increased volumes that come with a more accessible service;
- The ability of a national programme to lever relationships with other national agencies, such as the CPS.

We can draw the following key lessons from case studies A to D:

- Technology programmes should have clear, realistic objectives shared between commissioners, suppliers and users.
- Technology programmes should be user-led so that they can be co-designed with those who do the work, rather than imposed top down on the user base. As one interviewee told us,

> *"Don't force something on your users and then rush to a deadline".*

- Do not attempt to *'boil the ocean'* by seeking to replace everything all at once. More modular and gradual approaches are generally more realistic and flexible.
- Large ambitious programmes can leave customers reliant on monopoly suppliers who they are compelled to pay even when the programme is overrunning or not performing.
- Programmes driven mainly by cost or political imperatives rather than operational requirements or technical reality are likely to fail.
- Programmes should not be based on unrealistic or untested assumptions about what is technically possible.
- Using reliable off the shelf technology, and adjusting working practices to make use of it, is preferable to designing very bespoke (and therefore expensive) solutions, which try to make the technology fit existing ways of working.
- A final implication for UK policing IT programmes is that having the Home Office act as both the commissioner and ultimate provider of a programme is in the words of one police technology leader

> *"a weird relationship, a weird dynamic"*

with muddled governance and accountability. It is also better to have those who understand the operational requirements and who are closer to the work to design and deliver technology programmes. This means that ideally these programmes should be run by the police service itself rather than the Home Office.

POLICE

3. THE BARRIERS TO DATA-POWERED POLICING

So, what are the barriers to data-powered policing? What is preventing police forces from getting the right information into the hands of officers and staff at the right time? What are the barriers to the public receiving the same kind of seamless digital experience they receive in many other parts of their lives in their interactions with the police? In what follows we identify eight barriers to unlocking the power of digital, data, and technology in policing.

3.1 CULTURE AND MINDSET

Interviewees highlighted several cultural factors that they felt held policing back from making the most of data:

- Short termism and a lack of focus on the future.

> *"There's a lack of imagination". "We're always fighting yesterday's war, never focusing on the next threat."*

- So-called 'magpie syndrome', whereby police leaders focus on the 'shiny new thing' rather than thinking strategically about information and how using it more effectively could transform their business.
- Risk aversion with technology being seen as a source of risk rather than opportunity, leading to an unwillingness to innovate in case this disrupts core legacy systems.
- An unwillingness to learn from elsewhere, particularly from other industries or sectors where technology is at a more advanced stage of deployment.
- Perhaps underpinning all of the above is what was described as

> *"a lack of technological literacy among senior police leaders"*

and a failure of those leaders to surround themselves with the right expertise. One national police technology lead asked,

> *"How many forces have a technology person on the senior management team, at chief officer level? I can think of three."*

One chief constable considered the emphasis on technology in the Executive Leadership Programme, and its predecessor the Strategic Command Course, to be too weak:

> *"As chief officers we get very little training in this. Very few days on the ELP are afforded to the topic and that says a lot about where we are as a service."*

3.2 MARKET STRUCTURE

One police leader told us that,

> *"the structure of the market is a problem, with too many specialist requirements, a small number of cottage industry suppliers and a lack of competition".*

An experienced police procurement leader told us that this was true not just of technology but of police procurement generally:

> *"In too many areas there's a monopoly…with Airwave, there's one supplier, with Taser obviously, with body armour there are very few suppliers, in the vehicle market too."*

There are two possible reasons for these uncompetitive markets. The first is the specialist and highly regulated nature of police work. This means that they can only purchase technology and equipment that meet certain operational requirements or are compliant with strict standards. Only a small number of suppliers are able to meet these requirements producing monopolistic and uncompetitive markets.

Another explanation is that the police are culturally wedded to look for bespoke products. As one senior police officer told us,

> *"We have a tendency to bespoke everything, to want everything a particular way."*

This process of tailoring makes products more expensive than simply purchasing technology and equipment 'off the shelf'. Of course, there will always be specific policing needs that need to be accommodated within any solution, but arguably this is a matter of degree and many of our interviewees felt that the police tend to make excessive demands that add cost and complexity.

3.3 PROCUREMENT

Many industry representatives felt that police procurement processes were simply too complex and protracted. Examples were provided such as the setting of insurance requirements at such a high level that it is impossible for small and medium sized enterprises (SMEs) and start-ups to comply.

A police procurement lead responded that

> *"we are a complex and highly regulated environment".*

Whatever the cause of lengthy procurement processes, they have a number of consequences:

- They crowd out SMEs who find it too difficult to comply, locking the police to legacy providers who

  > *"cost more and are less innovative though also look less risky".*

- They are so protracted that by the time they conclude, the technology will have moved on.

  > *"They separate the person who has a problem and wants it solved from the person with the budget and who makes the decision."*

  So, suppliers spend valuable time with operational leaders developing a proof of concept and then find the project falls short when it comes to procurement.

- They act as a block on 'art of the possible' conversations simply because once a procurement starts police leaders are not permitted to talk to potential suppliers.

- They contribute to the so-called 'valley of death' problem discussed below.

We should note that the 2023 Procurement Act should help to speed up procurement processes by creating a central digital platform for suppliers to register and store their details so that they can be used for multiple bids and see all opportunities in one place. Commercial frameworks will also be made more flexible and the government says a number of bureaucratic barriers will be removed, benefitting start-ups and SMEs in particular.

3.4 THE VALLEY OF DEATH

One of the most significant positive changes in recent years has been the development of a more structured and strategic approach to innovation in policing, through the office of the Chief Scientific Adviser to Policing (see Case Study E). Most interviewees thought that there is now plenty of innovation being funded in policing, from data redaction tools to more advanced deployment of drones, but the problem is getting from the discovery phase, perhaps within a single local force, to the next step of scaling up for more widespread deployment.

This problem is typically known in science and business as 'the valley of death', which is when the funding for the initial discovery work has run out but companies or the government are not willing to fund further development because they are not sure it can scale. It is also often true that only a small proportion of a market is willing to try something completely new, which is not large enough of a market to make it profitable.

This problem was echoed in our interviews with SMEs who said

> *"the risk tolerance is just not there".*

Another said

> *"stuff will get momentum in discovery, but the process for moving forward is really difficult. We can have a six week discovery phase and then we've lost the money. And that's also when you involve legal and commercial."*

A key missing element in the police market is any clear framework for taking innovations that have been tested locally and then assuring them for the wider market so they can be deployed at scale. We return to this challenge in the next chapter.

Case Study E. The Office of the Chief Scientific Adviser to Policing

In May 2021 Professor Paul Taylor was appointed as the first Chief Scientific Adviser (CSA) to Policing. The role of the CSA is to promote and use emerging evidence, research and innovation in science and technology, including in both data and behavioural science, to advise policing on both the opportunities and risks to help reduce crime.

The CSA provides advice to police forces, the National Police Chiefs' Council (NPCC), the College of Policing, the National Crime Agency, the Association of Police and Crime Commissioners and others.

The CSA's objectives are:

- To connect science and technology expertise both in the UK and globally to keep policing at the forefront of best practice.
- To develop a science and technology strategy for policing, bringing coherence to the landscape and accelerating progress.
- To provide insight and solutions across policing, the criminal justice system and government with the aim of transforming the prevention and reduction of crime.
- To represent policing in the government's Chief Scientific Network, identifying cross-department opportunities and ensuring policing priorities are represented.

There is now a Science and Innovation Coordinating Committee of the NPCC and a Science and Technology Strategy. That strategy sets out a much more structured approach to innovation in policing, including the articulation of an end-to-end system for using science in policing, from innovation to deployment and evaluation. It also sets out a process for determining which innovations should be prioritised for further development.

Among our interviewees there was general praise for the CSA role and how it has been developed by Professor Taylor. As one said,

> *"there is now a more structured approach at the innovation end of the system."*

Many interviewees remained concerned about the scaling up of innovation and whether policing has a robust enough framework for doing that. We return to that question in the next chapter.

3.5 A LACK OF SPECIALIST SKILLS IN THE POLICE WORKFORCE

Shifting to a data driven approach is not just about technology, it is also about people, and it was clear from our research that there are concerns about whether the police workforce contains the specialist expertise to support its data and technology aspirations.

Examples of the types of roles required include data analysts, data scientists, AI specialists and technical architects. As one interviewee told us *"There's a lack of know how in policing. There's just not enough people with a real understanding of this technology."* This means that policing struggles to express clearly what it wants the market to provide and is not always aware of the 'art of the possible'. At the other end of the spectrum, policing does not always make full use of the technology it has purchased because its workforce has not been properly trained in its use. Interviewees described bits of software and equipment that are purchased but never used. A number of people told us that contracts should include more time for support and mentoring so that the police can get the most out of new capabilities.

One of the major challenges in terms of attracting skilled people is the fact that policing struggles to compete on salary with the private sector, who also need these same digital skills. They also compete with other public sector bodies who are also looking for those with data and technological expertise. We turn to how to tackle this in the next chapter.

3.6 BUDGET

Technology requires investment, but police funding is always limited. Several problems with the current system for funding police technology were highlighted:

- Funding is too short term and tends to stop and start owing to changing political priorities. Sometimes funding can be cut off before a programme has reached its full potential.
- There is often funding for innovation but less for scaling up and deploying new technologies.
- Technology is expensive. One former Chief Information Officer told us that

> *"chiefs are often surprised when they see the cost of cloud-based solutions. It will save you time and make better use of your officers, but the cost is there."*

Another interviewee told us, in relation to the challenge of achieving greater inter-operability,

> *"It won't be quick, it'll be a 10-year programme, it's going to take billions of pounds, but unless we do it the gap between policing and other sectors is going to continue to grow."*

- Sometimes investment in technology is seen as a way of saving money, but while technology may improve services and allow forces to shift resource by saving time, it is unlikely to result in cashable savings because of the almost infinite level of demand for policing. What it can do is make policing more productive in using the budget it has.

3.7 ORGANISATIONAL FRAGMENTATION

The biggest single barrier identified by our interviewees and our steering group is the organisational fragmentation of policing. As one interviewee put it,

> *"The 43 force model works against getting things done in this area. It has been overlayed by PCCs, who will fight their corner, because…they don't want to lose control and the Home Office retreating from having any direct involvement has made the situation worse."*

Another similarly argued,

> *"It's a governance issue. It is nuts and nigh on impossible to get things done through the 43 forces. There are some honourable exceptions but you have 43 sets of chiefs and forces all looking out for their own interests. And then you layer on PCCs who control the funding."*

In her recent Police Foundation lecture Dame Lynne Owens said that

> *"I have yet to hear a single rational reason why 43 different approaches to IT and infrastructure investment is sensible."*

The consequences of this organisational fragmentation include:

- Multiple data controllers who will set their own tolerances around sharing data.
- Different forces purchasing their own core systems at different times, and entering data in different ways, making data sharing difficult.
- A localised approach to the recruitment of specialists in highly competitive fields which arguably will never work.
- 86 veto holders when it comes to getting agreement to collaborate through national programmes. In the absence of a clear expectation from the Home Office this makes it impossible to develop a consistent and binding national framework in areas like data standards and the development of shared national solutions.

3.8 A WEAK CENTRE

In addition to the local fragmentation described above, the centre in policing is weak and confused. There is no clear governance nor a single strategy to direct digital and data policy nationally. We have a complex mix of programmes and strategies all with different lines of accountability to different people.

This confused picture includes:

- The major police IT programmes and databases owned by the Home Office.
- The Digital Data and Technology (DDaT) Coordination Committee chaired by Chief

Constable Rob Carden, with its four sub-boards and overseeing programmes including the new Centre for Data and Analytics in Policing.

- The Police Digital Service (PDS), accountable to Police and Crime Commissioners, which hosts the National Police Capabilities 'Environment'.
- The new Policing Productivity Centre based in the College of Policing, which will include an important data element.
- The Science and Innovation Coordination Committee chaired by Chief Constable Jeremy Vaughan.
- The Home Office National Crime and Justice Lab.
- Bluelight Commercial which is developing national procurement frameworks to maximise economies of scale.

There are too many bodies involved in police data and technology at the national level, and none of them have the power to properly coordinate behaviour locally. It is like an orchestra with six conductors.

One interviewee described the national system in the following way:

> *"The national space has out of date capabilities, managed in silos, risky and expensive, with no central strategy and no empowerment."*

Another said,

> *"we need a national approach, with a visionary approach from government and the threat of a stick….we need to mandate."*

Another added,

> *"It needs more of a push from the centre and for the Home Secretary to use her powers and lean in."*

One chief constable summed up the problem in the following way:

> *"The biggest issue is decision-making. 43 forces all making decisions about investment is not a model that is good for…best value. PCCs have local agendas. No one got voted in saying they are going to invest in really good technology. This model is not conducive to making strategic decisions for the service around key enablers like technology."*

They added:

> *"Currently there are lots of fingers in the pie. PCCs, Home Office, chiefs. The NHS don't have the Department of Health hosting their technology."*

POLICE

4. WAYS FORWARD

This report has described a police digital and data landscape that is struggling to unlock the power of information to drive better policing. Too much police technology is outdated, the police are burdened with siloed legacy systems, data is often of poor quality and inconsistently collected, and it is difficult to share information when so many of the core local systems do not speak to each other. It has also highlighted some case studies which have generated useful lessons as to how to undertake big technology change programmes in policing.

It has identified a number of factors that explain the state of police data and technology, from a lack of technological literacy among senior police leaders through to a weak national centre.

This chapter sets out several recommendations to help unlock the power of information in policing.

Recommendation 1: A single national enabling body for police digital, data, and technology

The biggest barriers, according to our interviewees, rest in the areas of organisation and governance. The system is too fragmented and the centre is too weak to create a clear framework in which local forces can operate effectively. There are too many bodies at the centre, with overlapping remits and none of them have any real powers to drive change locally. This was one of the main findings of the Police Foundation's Strategic Review of Policing, chaired by Sir Michael Barber, which reported in 2022.[2]

Elsewhere the Police Foundation has argued for a single National Police Headquarters which would bring together most of the disparate national institutions in policing into a single national home for policing in England and Wales with clear governance and a single strategy.

How encompassing such an organisation should be is a matter for debate, but at the very least it should be the body that hosts all national digital, data, and technology functions in one place.

This would mean:

- Incorporating the Police Digital Service (PDS), the NPCC DDaT (Digital Data and Technology) and Science and Innovation Committees and Bluelight Commercial within that National Police Headquarters.
- Reforming the existing NPCC Committees to form a single layer of governance in relation to digital, data and technology. Recruiting a full time national digital, data, and technology lead for policing, responsible for delivering a single strategy.

  What would this National Police Headquarters do in relation to digital, data and technology? It would:

- Implement a single national digital, data, and techology strategy across policing.
- Lead and coordinate all national policing technology programmes. This would include the transfer of the current major Home Office programmes.
- Host the new data and analytics centre.
- Have powers delegated to it by the Home Secretary to set mandatory standards around data quality and data sharing and to require forces to adopt nationally agreed solutions where necessary.
- Have responsibility for developing the knowledge and skills required throughout the police workforce. It might also provide a platform to recruit specialists with pay scales and progression pathways that are hard to achieve at local force level.

[2] See https://www.police-foundation.org.uk/policingreview2022/wp-content/uploads/srpew_final_report.pdf

- Put in place national blueprints and procurement frameworks for technologies that have been tested and assured to the right standards.

Recommendation 2: National procurement frameworks to enable the scaling and deployment of new technologies

Local forces should be the test beds for innovative technologies in policing. They provide a crucial access point to the police market in particular for SMEs and start-ups. However, to overcome the 'valley of death' problem we need the national enabling body to do the following:

- Coordinate funding to allow promising innovations to be scaled up so that they can be made ready for wider deployment.
- Provide a test and assurance function for these products so that local forces know they are reliable and meet the required standards. This has to be done once for the whole country rather than 43 times.
- Put those products on national procurement frameworks, meaning that the procurement process can be undertaken once for the whole country. In some cases there would be one product, but forces could choose when to adopt it and to what degree of functionality. In others forces might be free to select between a number of assured products."

Recommendation 3: A stronger partnership with the private sector

It is important that procurement processes are fair and impartial. However, it is also important that there is an open and constructive dialogue between the police and industry. It is only through such a dialogue that policing will be able to understand the 'art of the possible' in terms of technological innovation and it is only through dialogue that industry will understand the operational needs of policing.

There are some measures that might help to bridge the gap between the different sides of the marketplace:

- The use of trade bodies such as techUK to facilitate pre-procurement and early engagement conversations, as well as facilitating more strategic conversations between policing and industry and sharing good practice.
- The development of sandbox environments in which the police can share challenges and data, including synthetic data, to then allow businesses to test solutions in a safe environment prior to procurement.
- Mentoring by suppliers could be built into contracts so that officers and staff can be properly trained in the implementation of new technologies.
- Making more use of police volunteers from the private sector with specialist skills that policing needs but struggles to recruit directly.

Recommendation 4: A national strategy to promote interoperability

One of the goals of a new national enabling body should be to develop a strategy for interoperability, to overcome probably the biggest technical barrier to the sharing of information around the system.

As we have seen with the failures of major national IT programmes the last thing we need is the imposition of single national core systems on forces. Such a programme would no doubt be costly, would alienate local stakeholders and would risk repeating many of the design failings we saw with ESN and LEDS. Our interviewees stressed that such a single solution model is at any rate unnecessary.

Alternatives to this include:

- Encouraging further the regional federation of core systems, as we have seen with local forces in some regions joining together to develop shared records management systems for example.

- Encouraging the use of cloud-based integration platforms, which means that the different legacy systems do not need to speak to one another, but rather they can all speak to the integration platform. This also provides oversight and control of where the data is going and who can have access to it.
- Setting mandatory data standards which could over time promote direct interoperability between systems. This will not be straightforward and may not be necessary for all police systems. But it may be a good way forward for key data that needs to be regularly shared across organisational boundaries.
- Common data repositories, where data is pulled from different sources into a common space. This may be an option for historic data and is essentially the PNC model.[3]

Recommendation 5: A review of the data protection legislation that governs this area of work

We heard a high degree of concern about the barriers to progress created by data protection legislation. One chief officer commented that this legislation had almost made him give up on a major technology programme. The government should undertake a review of this legislation to understand the degree to which it is blocking technological innovation, not just in policing, but across the public sector.

Recommendation 6: Developing specialist skills within policing

Policing has a challenge in attracting talent within a highly competitive marketplace for digital and data skills. And yet policing desperately needs data analysts, data scientists, AI specialists and others if it is to make best use of the information it holds.

The following measures ought to be considered:

- Developing common job descriptions and progression pathways for digital specialists in policing.
- Collaborating with other government sectors and services to share specialists from within a central pool.
- Undertaking more specialist recruitment nationally.
- Promoting secondments for police officers and staff in industry.
- Mobilising police volunteering in this space, as has taken place through the Cyber Specials programme.

Recommendation 7: Developing greater technological and data literacy among senior police leaders

Overcoming some of the culture and mindset issues highlighted will require senior police leaders who understand technology and the role that data can play strategically in everything the police do.

This can be promoted by:

- Ensuring that there is a strong data and technology component to the Executive Leadership Programme.
- Encouraging the inclusion of Chief Information Officers or Chief DDaT Officers in chief officer teams so that those who understand technology are at the table when big strategic decisions are made.
- Promoting secondments of chief officers into industry.
- Achieving greater accountability through the inspection process. Digital maturity should be a core area within the PEEL inspection framework. There could be a new HMICFRS framework for DDaT assessment and it could become impossible for a force to be rated as outstanding if they do not attract a minimum score.

[3] Tech UK's Justice and Emergency Services Programme has established an Interoperability Working Group and I am grateful to them for sharing their emerging findings.

POLICE

5. CONCLUSION

Policing is at an inflexion point. The potential is clearly there for the way the police work to be transformed if the right information can be put in the right hands at the right time. That should lead to less harm, a greater proportion of crimes prevented and detected and a police service that is able to spend more time out and about engaging with communities.

However, in order to seize this opportunity policing needs to overcome several challenges. It needs to foster a true digital culture characterised by continuous learning, an emphasis on digital literacy, and the integration of technology into core operational activities. The police need to get their data moving around more easily so they can enable interoperability; they need to make sure their senior leaders really understand the power of information and what is required to enable it; they need to shift away from such a high degree of spend on legacy systems by embracing open solutions in the cloud and doing more at scale; they need to speed up procurement processes so that new technology can be deployed more quickly throughout the service; they need to be more imaginative about attracting the specialist skills they need and they need a more open relationship with industry.

Police leaders must champion innovation, encouraging a mindset shift where technology is seen not as a barrier to change, but as a critical enabler of more effective policing. Critically they need to resolve the collective action problem that is undermining their ability to make the most of the technological revolution. This means a single national enabling body with a clear strategy and simple governance. This should allow local innovation to flourish while creating a framework for scaling promising ideas and getting them deployed more quickly into policing.

The good news is that none of this is impossible. With a supportive political environment, buy in from across the service and clear national leadership, the police service can unleash the power of information.

REFERENCES

BBC (2009) The Famous Captain. *BBC.co.uk,* [online] 21 January. Available at: <https://www.bbc.co.uk/nottingham/content/articles/2009/01/20/chief_constable_popkess_feature.shtml>

Critchley, TA (1978) *A History of Police in England*. London: Legend.

Davies, G. (2021) *The National Law Enforcement Data Programme*. London: National Audit Office.

Davies, G. (2023) *Progress with delivering the Emergency Services Network*. London: National Audit Office. Available at: <https://www.nao.org.uk/reports/progress-with-delivering-the-emergency-services-network/>

Hillard, D. (2023) *UK Emergency Services Network fiasco – have we crossed the Rubicon?*. TelcoTitans. Available at: <https://www.telcotitans.com/infrawatch/uk-emergency-services-network-fiasco-have-we-crossed-the-rubicon/7029.article>

Kilburn-Wilson, S. (2023) How Colin Pitchfork was first murderer convicted using DNA fingerprinting after killing two girls.ITV.com [online] 7 December. Available at: <https://www.itv.com/news/central/2023-12-07/colin-pitchfork-the-day-dna-fingerprinting-convicted-its-first-murderer>

NPCC/APCC (2020) *National Police Digital Strategy.* London: NPCC/APCC. Available at: <https://pds.police.uk/wp-content/uploads/2020/01/National-Policing-Digital-Strategy-2020-2030.pdf>

Email: info@police-foundation.org.uk

www.police-foundation.org.uk

Charity Registration Number: 278257

THE
POLICE
FOUNDATION
The UK's policing think tank