Original Article

What does the UK Police National Database tell us about the future of police intelligence?

Rebecca Phythian[*] and Stuart Kirby[**]

Abstract Developments in technology are transforming society, creating more opportunities for offenders and complicating the policing landscape. The challenge for law enforcement is to identify criminal patterns from an offender's electronic traces and to provide actionable intelligence. However, these traces are held by diverse police forces and are rarely connected. In 2011, to overcome this challenge, the Police National Database (PND) was launched to provide a national intelligence overview from local data. This study examines the database, using a mixed-methods approach. Descriptive and inferential analyses of PND usage data highlight that different forces use the PND, and its various capabilities, with different levels of frequency. Thematic analyses of interviews and focus groups with PND users identified: specific examples of PND use, as well as its perceived strengths, perceived deficiencies, and future considerations. Implications for policing practice are discussed.

Introduction

The latter part of the 20th Century saw rapid social change, epitomized by mobility which became faster and less expensive. The advent of the 21st Century saw the speed of change intensify, characterized by developments in technology and digitization. During this period, the physical and virtual environments started to merge (Schwab, 2015), which led to the rise of smart cities, smart devices, and the development of cryptocurrencies. In contemporary society, an individual can organize much of their personal and business life via their smartphone, 24 hours a day.

These transformative changes are also exploited by offenders, which has ramifications for law enforcement agencies. Routine Activity Theory (Cohen and Felson, 1979) argues that crime occurs through the national rhythms of everyday life; therefore, 'crime is the intentional consequence of unintended opportunity' (Tilley, 2005, p. 266). Recent developments allow offenders the opportunity to travel further and more quickly, whilst the online environment can be used to maintain anonymity and facilitate crime. While legitimate digital assets (i.e. 'meme coins' or 'non-fungible tokens') grow, so do illegitimate actions, especially during the pandemic which has seen online fraud surge (Stripe, 2021). This technology can also be exploited by the police, to identify and target persistent offenders and reduce the vulnerability of repeat victims. However, whilst this course of action is simple in theory, it is more difficult to achieve in practice. Although offenders leave physical or electronic traces concerning their movement and interactions, these are disparate and fragmented, held by different police forces on various intelligence systems (Egbert, 2019).

[*]Senior Lecturer, School of Law, Criminology and Policing, Edge Hill University, Ormskirk, UK. E-mail: phythiar@edgehill.ac.uk
[**]Emeritus Professor, School of Justice, University of Central Lancashire, Preston, UK

Policing, Volume XX, Number XX, pp. 1–14
doi: https://doi.org/10.1093/police/paac074

These shortcomings were tragically highlighted in 2002 in the UK, following the murders of 10-year-old Holly Wells and Jessica Chapman. The offender, Ian Huntley, was known to various UK police forces for burglary, sexual and violent offences. However, due to the inability of police forces to link or disclose this intelligence, Huntley was able to acquire the post as their school caretaker and gain their trust. To prevent this re-occurring a government inquiry, led by Lord Bichard between 2003 and 2006, recommended the urgent development of 'a national information technology system for police intelligence in England and Wales' (Bichard, 2004, p. 13). From this emerged the Police National Database (PND), a system which allowed the 43 forces of England and Wales, the Police Service of Northern Ireland, British Transport Police, Police Scotland, and other national law enforcement agencies (e.g. National Crime Agency, the Child Exploitation, and Online Protection Centre) to share information 'to support public protection' (Lambri *et al.*, 2011, p. 5). The system was independent to the Police National Computer (PNC), which enjoyed mainstream access and usage. However, the PND linked 230+ local crime, custody, domestic abuse and child abuse records, allowing a more holistic intelligence picture concerning people (e.g. offenders), objects (e.g. stolen property), locations (e.g. address), and events (e.g. a crime report). Launched in 2011, it aimed to: safeguard children and vulnerable people; counter-terrorism; and prevent and disrupt serious and organized crime (SOC). Whilst one academic study explored its introduction (see Lambri *et al.*, 2011), there has been a lack of independent published studies to examine its progress and efficacy. Indeed, the success of such an enormous undertaking was not guaranteed due to the number of reports that show the introduction of police technology is fraught with challenges (e.g. Lum *et al.*, 2017). This specific study, therefore, explores the lessons that can be learnt from the PND, a decade after its launch.

Literature review

In an information-rich world, during periods when public resources are finite, it appears obvious that technology can improve police efficiency (Rutgers and van der Meer, 2010). Indeed, information technology (IT), which enables the harvesting and analysing of intelligence, is thought to be central to criminal investigations (Hollywood and Winkelman, 2015; Koper *et al.*, 2014; Weisburd *et al.*, 2003). As offenders often come to the attention of numerous agencies, multi-agency working and data sharing are fundamental to working practice (Carter *et al.*, 2014; Home Office, 2014, 2018; National Crime Agency, 2014). Whilst all information systems are introduced with the 'intention of making officers more efficient, fair and productive' (Carr, 2017, p. 360), this is 'easier to say but harder to do well' (Wilson and Gray, 2015, p. 5). The academic literature confirms the challenges in introducing, embedding, and using new technology (Lambri *et al.*, 2011; Lum *et al.*, 2017). This is because any organizational change, facilitated by IT, needs to go much further than the product itself (Lambri *et al.*, 2011).

Barriers to information sharing

There are various elements that generate these difficulties. At the outset, there are considerable technical challenges in designing software that can harvest data from disparate systems and provide a secure and user-friendly interface to analyse the contents (Wilson and Gray, 2015). These issues are exacerbated by the lack of consistent data standards (Evans-Pughe, 2006; Hollywood and Winkelman, 2015), which leads to inaccuracies in the recording of 'people, events and even colours' (CGI, 2013, p. 1). Difficulties also surround the need for a secure system that complies with legal requirements (Lum *et al.*, 2017; O'Neil, 2017), as well as numerous concerns between partners over proportionality, legal ambiguity, and appropriate guidance (Thomas and Walport, 2008).

The fear of what can and cannot be legally shared can result in practitioners failing to reveal, or over-sanitize, information rather than risk data protection breaches (Pinkney *et al.*, 2008; Wilks, 2014). This is compounded by concerns that other agencies will fail to manage the data according to legal and procedural guidelines (Dawes *et al.*, 2009; Wilson *et al.*, 2011). In fact, it is argued there is a 'fog of ambiguity and uncertainty surrounding the

legal framework' (Thomas and Walport, 2008, p. 40), which leads to risk aversion, poor data sharing, and ultimately detracts from proactive approaches to tackling crime (Thomas and Walport, 2008; Van Staden *et al.*, 2011). This is intensified when the data are particularly sensitive in nature (Kirby, 2013).

Police organizational culture is also highlighted as a major obstacle to organizational improvements, which include technological change. Lambri *et al.* (2011, p. 10), specifically argued the way PND challenged existing cultural norms, 'could in fact impede the evolutional development', and cause officers to block its use. These cultural aspects are exacerbated in multi-agency work. This is because different agencies are more likely to generate conflicting cultures (Barnes, 2008; Horwath and Morrison, 2007), competing priorities (Atkinson *et al.*, 2005; White, 2009), different attitudes to information sharing (Hollywood and Winkelman, 2015), institutional friction (Gillen, 2011; Pratt, 2012; Stanier, 2013), and logistical challenges (e.g. funding, space, compatible technology; Atkinson *et al.*, 2005; Barnes, 2008; White, 2009). Other issues, such as poor leadership, limited resources (funds and IT), and a lack of engagement with innovation are also said to hinder an intelligence-led approach (Darroch and Mazerolle, 2013; Ratcliffe, 2005, 2008; Sanders *et al.*, 2015). Deloitte (2015) discovered in their survey that over 80% felt employee resistance was the main cause of technology projects failing; a finding previously reported by others who have uncovered active resistance from police officers (Ericson and Haggerty, 1997).

Facilitating effective information sharing

Understanding the barriers to successful implementation can provide the means to ameliorate them. In relation to the technical issues, it assists if practitioners can work closely with developers to identify appropriate technology requirements (Deloitte, 2015; Hollywood and Winkelman, 2015). Lambri *et al.* (2011) emphasize the importance of understanding how practitioners interpret the data from the IT system rather than just focusing on the technology. Ultimately the importance of collaborating with end users during the initial development stages has been recognized as 'fundamental to the successful delivery of … technology programmes' (House of Commons, 2021, p. 3).

Several commentators have suggested the way to reduce cultural resistance is through business processes and business change (Lambri *et al.*, 2011). Neyroud and Disley (2008, p. 230) highlight the importance of 'management and oversight' when dealing with new technology, arguing effective governance requires an emphasis on four issues: (a) *integrity*—specifically the security, accuracy, and reliability of the system, with clear governance over how the information is shared with other agencies; (b) *outcomes*—which understands 'the value added … to various aspects of policing' as well as the involvement of independent research to make this clear; (c) *transparency*, relating to how systems and databases are governed; and, (d) *public confidence* and trust in the new technology.

Thomas and Walport (2008, p. 59) also endorse the importance of 'strong leadership and clear lines of accountability' when sharing information, with Koper *et al.* (2014, p. 215) arguing that 'management practices, agency culture, and other contextual factors' play an important role. This can be assisted by mainstream acceptance of innovative technology, coupled with training, technical support, and incentives (Lum *et al.*, 2017). In fact, the absence of training associated with new technology can often make new systems irrelevant (Martin and Jackson, 2008). It appears when technology is endorsed by other organizational changes it is linked with enhanced performance (Garicano and Heaton, 2010; Willis *et al.*, 2007).

The current intelligence landscape and developments in the PND

As is illustrated later in the paper, the PND has evolved from its original purpose of providing a national police intelligence system, that provided a national view of local force data (holding intelligence on people, objects, locations, and events), to also act as a national information source for organized crime and organized crime groups (OCGs), including county lines, modern slavery, and human trafficking. It has undergone technological developments (i.e. improved facial searching) and supported

multiple pilot programmes (i.e. firearms, domestic abuse non-molestation orders). However, following the launch of the National Law Enforcement Data Service (NLEDS) programme in 2016, there has been 'repeated deferral of investment mean[ing] that some elements of the PND's infrastructure have reached the end of their service lives, affecting both service quality and stability' (National Audit Office [NAO], 2021, p. 33). Subsequently, in December 2020, the Home Office decided to maintain the PND 'as a standalone system until 2031', with renewed investment and development in the PND underway (NAO, 2021, p. 6; Say, 2021).

Summary

In summary, although the PND was introduced in response to a failure by UK police forces to share information, this type of intelligence failure occurs across the world (Kirby and Keay, 2021). The PND was therefore implemented to make available 'the wealth of information held, but not exploited, by police forces for the prevention and detection of crime' (Bichard, 2004, p. 130). This meant tackling the incongruent technology systems across different police forces which, 'led to real difficulty in accessing all relevant information, which has in turn resulted in poorly informed decision making' (ibid, p. 129). However, as explained by the National Police Improvement Agency (NPIA, 2009, p. 7), the PND project 'is not just an IT project; it is helping the Police Service to deliver fundamental business change improvements enabled by IT'. As such, research can assist in adding to the contextual understanding of implementing and adopting police technology (Lum *et al.*, 2017), as 'police often adopt new forms of technology before their impacts and effectiveness have been demonstrated' (Koper *et al.*, 2014, p. 219). As the wider landscape shows, intelligence has a critical role to play in tackling current strategic policing priorities; for example, the violence against women and girls strategy underlines 'the importance of effective information sharing and clear data' (Home Office, 2021a, p. 75), with the significance of 'data collection and intelligence sharing' noted in the Beating Crime Plan (Home Office, 2021b, p. 31). Ensuring the effective use of the PND is therefore essential to support policing in protecting the public and tackling serious crimes.

Methodology

Access to police systems is often limited due to legitimate concerns surrounding the confidentiality of police operations. This study has been supported by both the users (UK National Police Chiefs' Council [NPCC]) and developers (CGI) of the PND. Care has been taken with this study not to identify any issues that may compromise operational capacity or capability, and the process has included the vetting of research staff, together with the anonymization of data.

The study uses a mixed-methods approach. The quantitative element explores numerical data to establish PND usage across the 56 British police forces and associated agencies (i.e. Home Office, National Crime Agency). Specifically, it examines the number of commissioned PND licenses ('enabled' and 'used', as of June 2019), as well as the number of searches across various categories (July 2018 to June 2019). The number of searches was counted in the following categories: *POLE* (a search relating to a person, object, location, or event); *facial* (a search of images of people held on the PND); *bulk facial* (a search of multiple images); *bulk* (a bulk search of other details); *scheduled* (a search scheduled to automatically occur at a set time: weekly, monthly, quarterly or annually); and *triggered* (a search scheduled to automatically run on a daily basis). All quantitative data were anonymized and transferred into SPSS to facilitate descriptive and inferential analyses. Shapiro–Wilk tests of normality deemed the data to be skewed ($P < .05$); therefore, non-parametric tests (i.e. Kendall Tau correlation) were conducted.

The qualitative aspect of the methodology involved semi-structured interviews and focus groups with individuals perceived to be experts in the system. The 17 participants were contacted with the aid of the NPCC PND lead, and further participants were recruited via a snowball sampling technique. Due to accessibility and scheduling, a variety of methods were used (during Spring 2019); 10 interviews (face-to-face or via the telephone), two focus groups (one

consisting of a group of two and a further consisting of a group of three), and two written responses. The roles of the participants included a Chief Police Officer with national responsibility for PND and senior police officers with managerial responsibility for the development or implementation of PND, as well as PND users, auditors, and administrators. The interviews were transcribed and anonymized. NVivo was used to conduct a thematic analysis of the data to establish the key themes, with quotes from the practitioners anonymized using reference numbers (i.e. P1, P2, etc.).

Whilst it is acknowledged the sample size was small, it is not dissimilar to other research examining expert perspectives (i.e. De Paoli *et al.*, 2021, n = 13; Olver and Cockbain, 2021, n = 11); the exploratory research offers valuable insight, including perceptions of those from a range of roles and agencies. Moreover, the practitioner interviews provide a contextual understanding and complemented the quantitative data on search usage.

Results

The results follow the quantitative and qualitative approaches as highlighted above.

Quantitative

As the system is separate to PNC all agencies which use the PND are required to purchase licenses, which enable its use. The number of required licences is specified by the individual agency, which is guided by personnel numbers and predicted use. The data show that although many licenses were commissioned, not all were activated; in June 2019, an average of 228.76 (SD = 207.69) licenses were enabled, compared to 137.11 (SD = 128.99) licenses that were used. The percentage of activated licenses ranged from 0% (which related to a small agency which had seven available licences but had not activated any of them) to 90% (median = 63%). At this basic level, it shows that the actual use of the PND does not match the potential availability. Kendall's Tau correlations between the size of the force[1] and both the number of licenses commissioned and activated were found to have statistically significant relationships, albeit of a moderate strength[2] (T = 0.578, P < .001; T = 0.555, P < .001, respectively); this indicates that, generally, the bigger the agency the more licenses that are commissioned and active.

In relation to individual search usage, again there were disparities between police forces (Table 1). Whilst some inconsistency could be expected, as the agencies cover widely different areas, it was shown that the POLE searches ranged from 0 (found within two agencies) to over three-quarters of a million in another agency. Similarly, the facial searches ranged from 0 in three agencies to more than 2,000 in another. This pattern was illustrated across all available search categories and it indicates that different police forces chose to use the PND, and its various capabilities, with different levels of frequency.

Table 1: Descriptive statistics: Search type (July 2018 to June 2019)

	Search type					
	POLE	Facial	Bulk facial	Bulk	Scheduled	Triggered
Mean (SD)	105,917.07 (113,753.14)	294.30 (426.31)	10.39 (27.08)	26,602.73 (37,974.77)	3,634.32 (12,926.99)	9,826.89 (44,224.73)
Median	76,853	126	0	15,474	58	461
Range	0–765,328	0–2,056	0–156	0–165,337	0–82,339	0–325,240
Total	5,931,356	16,481	582	1,489,753	203,522	550,306

[1] Based on 46 agencies in the sample, with force size figures obtained from Statista (2022).

[2] The correlation coefficient (T) indicates the strength of the relationship. A value of less than 0.35 is deemed to be weak, 0.36–0.67 to be moderate, and 0.68–1.0 to be strong (Taylor, 1990).

License use significantly positively correlated with each of the search types (i.e. as license use increases, so does search frequency), yet such relationships varied from a weak to moderate strength: POLE ($T = 0.548$, $P < .001$), facial ($T = 0.498$, $P < .001$), bulk facial ($T = 0.379$, $P < .001$), bulk ($T = 0.585$, $P < .001$), scheduled ($T = 0.363$, $P < .001$), and triggered ($T = 0.367$, $P < .001$). In relation to agency size, significant positive, albeit weak, relationships were reported with POLE ($T = 0.463$, $P < .001$), facial ($T = 0.357$, $P < .001$), bulk facial ($T = 0.325$, $P < .01$), bulk ($T = 0.248$, $P < .05$) and triggered ($T = 0.278$, $P < .01$) searches, yet scheduled searches did not correlate ($P > .05$). However, of note, when the two largest agencies were removed from the analysis, both bulk and scheduled searches were not significantly related to agency size ($P > .05$). Whilst such analyses highlight that, generally, the larger the agency and the more licenses used, the higher the frequency of various search types, the absence of *strong* associations between the variables should be considered.

Qualitative

This section provides results in four thematic areas: (a) specific examples of PND use; (b) perceived strengths; (c) perceived deficiencies; and (d) future considerations.

(a)*Specific examples* Participants provided a vast range of positive examples emanating from their use of the PND, highlighting its ability to assist in quickly apprehending an offender and finding a missing person due to facial recognition, initiating investigative leads, and offering a holistic view of an individual to inform the assessment of threat, risk and harm. To assist the reader with a wider understanding of the transformation the PND has made to intelligence analysis, four scenarios are selected:

> Example 1: "a vulnerable lady with young children, single parent, met someone online, formed a very quick relationship and that person committed sex offences within that family environment. But the only contact, or only evidential trace, was the photograph of the social media profile … that's run through PND and immediately identifies the person … they were arrested within hours. So that's the value of PND, not the potential value, the value because it happens all the time" (P4).
> Example 2: "[force] were dealing with a murder with a vicar in a church and the PND had information on somebody who had made a threat to kill members of the clergy. So, having done that search, the investigators realised it's probably the person they're looking for and it led them to an address. They found the person and blood-stained clothing in the wash, as he was trying to get rid of the evidence" (P7).
> Example 3: "When we were aware of [facial searches] we put a person's picture into the system that had been missing for 10 years … we found this person in 20 minutes" (P17).
> Example 4: "Vetting is better because now you have access to all of that data across the whole area, all forces" (P10).

(b)*Perceived strengths* Participants recognized the value of the PND, in terms of its innovation and ability to transform the intelligence, and policing, landscape. Benefits of the PND are captured according to three themes: (i) a consistent and reliable approach to intelligence; (ii) transforming police intelligence; and (iii) a holistic view.

i. A consistent and reliable approach to intelligence

As can be seen from the examples provided, participants explained the PND provided a step change to intelligence analysis, arguing that prior to the PND there was 'no intelligence sharing capability' (P13). Whilst some historic mechanisms, such as national intelligence bulletins, did exist these were 'not really effective at all' (P4). What previously existed was a haphazard approach, which was both ineffective and inefficient. For the police to establish if an individual was known elsewhere, an officer

sent requests to other forces in a variety of ways, such as 'general intel mailboxes' or 'a phishing email to all of the forces to clarify' (P11). One participant explained they would, 'go to 43 forces and say "tell me what you've got on [name]", unless I know where [name] has come from, it wouldn't be done' (P10). Ultimately police forces would respond arbitrarily, often ignoring the intelligence request or providing only limited information.

ii. Transforming police intelligence:

Participants explained the PND had transformed the intelligence process and met its remit in tackling terrorism, serious organized crime, and improving safeguarding. The system had also improved over time with P10 stating, 'When it first started … it was very clunky. You had to fill a form out and send it off ... Now its developed, you can access that data yourself, so you can go right … click on that force and give me that data. It's massively different'. This was endorsed by P13: 'When you look at where we started, and that we had nothing, it's been 100% successful…. It works. It solves murders, as well as volume crime, missing persons'. Practitioners pointed out it supported the intelligence picture on a daily basis, benefitting OCG management, operational planning, and major investigation. It was also said to be useful to a diverse range of departments and teams, including control rooms, intelligence teams, child protection, domestic abuse, and vetting. The participants recognized how the PND brought a new capability to the intelligence landscape:

> Historically with intelligence, it's always been an issue … around the ability to share information between border agencies, national agencies and policing. Along comes PND, you've solved it. (P4)
>
> To think of policing in the 21st century without a PND equivalent is just, you're back in the stone age. (P5)

iii. A holistic view:

Practitioners lauded its ability to provide a holistic picture. As P6 explained, 'everybody uses the PNC [Police National Computer], but the PNC tells you information you already know. I know you've been arrested … but I didn't know that he was talking to [name] … that he drove that car … had this phone number. Now, that's gold dust and that's where we should be working'. Furthermore, the system was acknowledged to be innovative, 'at Europol … they were amazed at PND. They were like "we don't have anything like this". So, we're in a really unique position … we've got something that we can really get some value from' (P12). The power of the system in providing a holistic understanding was summed up by P13:

> In [the PND] we have records of 16 million people. So that includes from a safeguarding perspective as well. Two million organisations, which can include OCGs. 85 million intelligence records, 160 million crimes records, 130 million custody records, six million child abuse records, 17 million domestic abuse records, 1.1 billion association records and there's no point having 4.1 billion records if they're not linked to tell the story. So, if you can't link the person to the child abuse record it doesn't tell the story. We've got 14 million searchable images from people who have come into custody, 14.4 million telephone numbers, 12,000 OCGs, and that's from 55 agencies and 250 sources.

(c)*Perceived deficiencies* Whilst the perception of the system was overwhelmingly positive it was agreed that improvements could be made, specifically surrounding three themes: (i) system design; (ii) system integrity; and (iii) system use.

i. System design:

Participants commented that the system was sometimes difficult to navigate, which increased the time spent on the system:

> I find navigating around all the different kind of searches quite clunky, it's

> not obvious where you'd look sometimes for information. (P1)
> It's a bit of a beast to use, I'll be honest, it's not massively user friendly, but if you consider the vast volume of data that it's dealing with, it's what we've got, and it bridges those gaps. (P3)

Speaking about the design, the need for a close relationship between software developers and practitioners was discussed:

> Decisions are made by people who don't understand the system and they get IT developers to do something who don't understand the system, so they'll say yes to everything … they do go out and they do speak to you, and then they write down what they think you said, and they'll go and give it to some programmer, but they won't give them the whole picture, they're just doing that one little bit of it. (P5)

Several specific technical improvements relating to search criteria and analytical tools were suggested to make the PND more user-friendly. Indeed, the importance of the practitioner–developer relationship extended into training:

> [the training questions] aren't built for a user, they're a test, like how bizarre a record you can find … that's not really what it's like…. All of it is based on the training system which doesn't have a volume of records in anyway, so it's not particularly representative of a search that you'd do to begin with. (P12)
> You'd ask the trainers questions but because they're not users, they're not really able to answer your practical questions. (P12)

ii. System integrity:

As the information is generated from forces all across the country, there was a further theme around national standards and consistency:

> All the IT systems are different, all the IT systems work differently, you're trying to feed them onto one database, which is a horrendous task. (P5)
> There's a real need ... to have a stronger national governance around data quality, data currency, for things like PND. (P4)

This even extended to the level of information input onto the system:

> Some forces will load next to nothing on it, but they're technically loading onto it. (P5)
> Issues around completeness and consistency of the data, as well as currency of the data. (P4)

However, as others explained this was an issue that affected all national systems and not just the PND:

> There'll always be an issue about data quality, but it's not the PND, it's the source of data. Some of it you can avoid and some of it you can't. (P6)

iii. System use:

There was a consensus that the system was not being used to its potential, leading to 'a lot of missed opportunity' (P11). Two specific explanations were provided to explain this. The most obvious reason was access limitation due to cost. As P8 reported, 'the barrier does tend to be the initial access and the amount of people who can have it. I'd love to give somebody on every single team access to it, but I can't'.

Resourcing was therefore an issue, ranging from the availability of terminals to limited time and staff (e.g. 'I'm not given the time or opportunity to do it' [P9]), to a much broader issue of funding. Overall, funding was seen to connect to everything, including the development of the system and the support for users: 'You don't want to say to people who want access to PND "you can't have access actually because it's going to cost you X amount"' (P5).

Furthermore, as searches were often done through specialist officers in central locations, its

use was reliant on officers being aware of the system and how to access it:

> You think, it's been out 11 years, why are we going around telling people the advantages of PND, surely you must know this and be doing it. (P5)
> The frustrating thing, people don't know what they have or how to make best use of it. (P13)

Participants suggested the lack of a systematic and centralized marketing approach leads to the differences in awareness across agencies.

The second explanation concerning its lack of use was that practitioners simply chose not to use it to its potential. A participant explained why this may be the case:

> I think the information sharing barriers that we come across are those with nervousness around sharing information … people worry … it's sort of a complex area of information compliance isn't it, and one that people are concerned about…. You can start to see a culture that is developing around being concerned around sharing information because of penalties and fines, and not really counterbalancing that with threat, harm and risk, information sharing practicalities in order to safeguard an individual. It is tricky, we're asking our frontline staff to be able to understand and interpret huge swaths of legislation and we need to make that easier for them. (P15)

This situation was frustrating to the interviewees:

> I will tell you something because I'd rather you be kept safe then end up being killed by somebody. And I can live with that. If I get my ass kicked for telling you data that I shouldn't have told you, ok fine. But I believe, we talk about dare to share, we still don't do it. (P10)
> What we have sort of forgotten in the background is I can point to serious case review after serious case review where actually, the common criticism is not sharing information and intelligence that could have made a difference in relation to a safeguarding activity, something that would've made a difference to that individual. (P15)

There were also wider cultural issues, such as trust:

> The dangers of not giving people access far outweigh the risks of them seeing the intelligence … it's part of your role, you're trusted, you've got vetting, it's a legitimate tool in your pack … using those tools with honesty and integrity, quite rightly code of ethics … for a policing purpose … as policing UK, we should trust our officers and our staff to access appropriately. We give our local systems, so why not the national system. (P3)

However, it was felt risk could be mitigated if the data being transferred into the PND was appropriately recorded by its owner:

> The more people who have access, yes of course there's more risk…. If the intelligence is handled properly by its home force, it will only be uploaded with a certain level of access anyway … then if you don't have the permissions, you don't have the permissions. (P3)

(d)*Future considerations* Finally, participants were provided with the opportunity to suggest how the PND should evolve in the future. There was a consensus that the system had much more potential and was currently constrained. One participant summarized the dilemma:

> What we also have is 20th century thinking, but when we've got 21st century technology and 21st century problems … how do we manage risk now, never mind in 2023 … it should be seen as a capability, not as an IT system. It's about how we transform policing….

> Offending is no longer local, not even across forces, they're now global…. When you take into account digitally, mobile world, digital world, we don't make good use of the technology we've already got … we have to think of new ways of working and technology to overcome all the issues. (P13)

Another participant suggested how the system could evolve,

> For me, in an ideal world, everybody would put onto PND. It's that one place to go to … that's where, for me, if you can pull in partner agencies, it's an even stronger tool … if everybody came onto one system, everybody would have that—if the world was on it, we'd have a whole system approach. (P10)

In this, the potential of including other existing databases was also discussed, from Driver and Vehicle Licensing Agency to Missing from Home information. A wider partnership was seen as a significant step forward:

> We've got to start engaging with the private sector and start engaging with international law enforcement because they have, their intelligence adds value to us and we have information that's of value to them, so we have to make sure there's the necessary safeguards. (P13)

Discussion

This research set out to understand the use of the PND, exploring the lessons that can be learnt from the system, a decade after its launch. The quantitative data highlighted instances of the failure of agencies to use all licenses issued, with great variations in both the use of the different search types and the frequency of use. This indicates the need of agencies to ensure they are utilizing the PND to its full potential. The qualitative data offer examples of how the PND has facilitated policing practice, as well as highlighting its perceived strengths and deficiencies, with practitioner suggestions of how the PND could be developed. Echoing earlier literature, these insights are critical at a time when the PND is undergoing investment and development. The implications of such findings will now be discussed.

The study generated four major themes that start with the general and move to the specific. The first point highlights the importance of independently reviewing data management systems. Such systems are significant both in terms of cost and central to police effectiveness and, during the past decade, problems have been reported. One issue relates to overpromising, such as an £80m commission of mobile data units, which failed in their undertaking to save 30 min for each officer, per shift (Berry, 2010). However, more problematic is when an information system fails. An example relates to the Athena information system, used by nine UK police forces at a cost of £35m. This faced significant implementation problems and became associated with allegations that it facilitated offenders escaping justice (Waterhouse, 2019). Even more recent was a northern police force that declared a critical incident following a failed upgrade of its £29m information system, which led to officers recording incidents on paper (Williams and Britton, 2020). The lack of independent evaluation is thought to be due to the operational sensitivity surrounding the systems, coupled with the absence of an evaluation culture (Kirby, 2013; Syed, 2015). Nonetheless, understanding the efficacy of an information system is vitally important if improvements are to be made. As recognized by the Head of MI6, offenders are constantly evolving, and policing agencies need to do the same, therefore they must engage with third parties to stay fit for purpose (Moore, 2021). Whilst it is accepted that this study has limitations, both in the level of quantitative analysis and the number of participants, it provides an independent and objective perspective from which improvements can be made.

The second point is that the study provides a proof of concept in relation to a new approach to information sharing. Law enforcement information systems, across the world, are often closely guarded (i.e. Pinkney *et al.*, 2008; Thomas and Walport, 2008; Wilks, 2014; Wilson *et al.*, 2011). This means that when partners need to share intelligence

systematically, as seen in US-based fusion centres or agencies such as Europol, representatives from the disparate agencies are brought together to access their individual systems independently and disclose information on request. The PND works differently. It brings together more than 230 databases from approximately 50 multi-jurisdictional agencies and supplies a user-friendly practitioner interface, which all agencies can interrogate. This is a critical finding as it shows diverse agencies can, in practice, pool different electronic data sources, held in different formats, to establish a more holistic picture of a person, object, location, or event (POLE). In a world where offenders are more likely to move quickly and leave traces across diverse jurisdictions, the benefits of this approach are enormous. If this unique concept was replicated more widely it could increase the level and quality of police intelligence and reduce cost in both police time (through individual police searches), as well as limit the need for extra intelligence structures.

Third, whilst practitioners unanimously endorsed the transformative benefits of PND and its ability to deliver a more holistic intelligence picture, the system could also be improved. As the academic literature has previously shown there are technological and organizational reasons why electronic information systems (less complex than the PND) fail (i.e. Hollywood and Winkelman, 2015; Pratt, 2012; Sanders *et al.*, 2015; Wilson and Gray, 2015). This study supports previous research and explains further the barriers and facilitators surrounding the implementation and use of information systems. Specifically, both the quantitative and qualitative data illustrate the PND was not being used to its potential and was inconsistent across police forces, both in terms of use and the level of information they shared on the system. Whilst associations between the size of the organization, the number of licenses enabled and used, and the frequency of searches conducted is expected, the correlations were of a weak to moderate strength, which were somewhat influenced by outliers (i.e. when the two largest forces were removed from the analysis, the relationship between agency size and bulk search frequency was no longer significant). What's more, the correlational analyses, varying in the levels of strength and significance, alongside the descriptive statistics, highlight inconsistencies in use (i.e. a number of agencies conducted zero searches in relation to a number of search types). The difference between forces is disproportionate and cannot solely be explained by the size of the organization. Practitioners explain the difference through several reasons which encompass the value they place in the approach, their resourcing of it, how risk averse they are (specifically over legislation), publicity of the system and training provided to their personnel. These issues relating to discretion, emanating from police organizational culture, have been widely discussed as blocking organizational change within policing, including the use of technology. This research endorses other studies that argue any technological-based change must be supported by other organizational change. This includes leadership, infrastructure, and supporting processes.

Finally, this study has also shown the tensions inherent in a national system which is born from local jurisdictions that enjoy individual autonomy and operational discretion. The database has highlighted significant inconsistencies, from practitioner commitment to data integrity (i.e. Evans-Pughe, 2006; Hollywood and Winkelman, 2015). This finding suggests a more fundamental change may be needed, should UK policing highlight the centrality of information sharing to the effectiveness and efficiency of their core business. This may affect work at street level, in understanding the electronic footprint of individuals who come to the attention of the police, including social media. This radical change would also be needed at a strategic level to improve compliance around data integrity and use of the system

In conclusion, due to increased digitization and the rise of technology, it is very difficult for offenders not to leave electronic traces of their actions as they travel across time and space (either physically or online). The policing challenge is to collect all the traces an offender leaves and identify the pattern that emerges, which presents actionable intelligence to protect victims or target offenders. The PND has shown that this concept can be achieved. However, if it is to evolve further it must be accepted that local data have national significance; therefore, it would be helpful to have national standards for data quality and PND use.

Acknowledgements

The authors would like to thank the NPCC and CGI for supporting this research. We would also like to thank all those who participated. The research was facilitated by internal pump prime funding (awarded to RP by the University of Central Lancashire's School of Forensic and Applied Sciences Research and Innovation committee).

References

Atkinson, M., Doherty, P., and Kinder, K. (2005). 'Multi-Agency Working.' *Journal of Early Childhood Research* **3**(1): 7–17.

Barnes, P. (2008). 'Multi-Agency Working: What Are the Perspectives of SENCos and Parents Regarding Its Development and Implementation?' *British Journal of Special Education* **35**(4): 230–240.

Berry, J. (2010). Reducing Bureaucracy in Policing: Final Report. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/117162/reduce-bureaucracy-police.pdf (accessed 16 February 2022).

Bichard, M. (2004). The Bichard Inquiry: Report. https://dera.ioe.ac.uk/6394/1/report.pdf (accessed 13 December 2021).

Carr, J. B. (2017). 'Estimating the Effects of Police Technology Using Quasi-Experimental Methods.' *Journal of Benefit-Cost Analysis* **8**(3): 360–368.

Carter, J. G., Phillips, S. W., and Gayadeen, S. M. (2014). 'Implementing Intelligence-led Policing: An Application of Loose-Coupling Theory.' *Journal of Criminal Justice* **42**(6): 433–442. doi:10.1016/j.jcrimjus.2014.08.002.

CGI. (2013). Police National Database. https://www.cgi-group.co.uk/sites/default/files/files_uk/casestudies/Case_Study_-_PND.pdf (accessed 13 December 2021).

Cohen, L. E. and Felson, M. (1979). 'Social Change and Crime Rate Trends: A Routine Activity Approach.' *American Sociological Review* **44**(4): 588–608. doi:10.2307/2094589.

Darroch, S. and Mazerolle, L. (2013). 'Intelligence-led Policing: A Comparative Analysis of Organizational Factors Influencing Innovation Uptake.' *Police Quarterly* **16**(1): 3–37. doi:10.1177/1098611112467411.

Dawes, S. S., Cresswell, A. M., and Pardo, T. A. (2009). 'From "Need to Know" to "Need to Share": Tangled Problems, Information Boundaries, and the Building of Public Sector Knowledge Networks.' *Public Administration Review* **69**(3): 392–402.

Deloitte. (2015). The Digital Policing Journey: From Concept to Reality—Realising the Benefits of Transformative Technology. https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/public-sector/deloitte-uk-ps-digital-police-force.pdf (accessed 13 December 2021).

De Paoli, S., Johnstone, J., Coull, N. et al. (2021). 'A Qualitative Exploratory Study of the Knowledge, Forensic, and Legal Challenges from the Perspective of Police Cybercrime Specialists.' *Policing: A Journal of Policy and Practice* **15**(2): 1429–1445. doi:10.1093/police/paaa027.

Egbert, S. (2019). 'Predictive Policing and the Platformisation of Police Work.' *Surveillance and Society* **17**(1/2): 83–88.

Ericson, R. V. and Haggerty, K. D. (1997). *Policing the Risk Society*. Toronto, Canada: University of Toronto Press.

Evans-Pughe, C. (2006). Share and Share Alike. https://crypto.stanford.edu/portia/media/ET_Nov06.pdf (accessed 13 December 2021).

Garicano, L. and Heaton, P. (2010). 'Information Technology, Organization, and Productivity in the Public Sector: Evidence from Police Departments.' *Journal of Labour Economics* **28**(1): 167–201.

Gillen, A. (2011). Multi-Agency Working with Children and Families: A Focus on Facilitators and Using Activity Theory Principles to Explore This Topic Area. https://core.ac.uk/download/pdf/40013293.pdf (accessed 13 December 2021).

Hollywood, J. S. and Winkelman, Z. (2015). Improving Information Sharing Across Law Enforcement: Why Can't We Know? http://www.rand.org/pubs/research_reports/RR645.html (accessed 13 December 2021).

Home Office. (2014). Serious and Organised Crime Local Profiles: A Guide. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/371602/Serious_and_Organised_Crime_local_profiles.pdf (accessed 13 December 2021).

Home Office. (2018). Serious and Organised Crime Strategy. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752850/SOC-2018-web.pdf (accessed 13 December 2021).

Home Office. (2021a). Tackling Violence Against Women and Girls. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1033934/Tackling_Violence_Against_Women_and_Girls_Strategy_-_July_2021.pdf (accessed 28 February 2022).

Home Office. (2021b). Beating Crime Plan. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1015382/Crime-plan-v10.pdf (accessed 28 February 2022).

Horwath, J. and Morrison, T. (2007). 'Collaboration, Integration and Change in Children's Services: Critical Issues and Key Ingredients.' *Child Abuse and Neglect* **31**(1): 55–69.

House of Commons. (2021). The National Law Enforcement Data Programme: Twenty-Ninth Report of Session 2021-22. https://committees.parliament.uk/publications/8125/documents/83326/default/ (accessed 28 February 2022).

Kirby, S. (2013). *Effective Policing? Implementation in Theory and Practice*. Hampshire, UK: Palgrave Macmillan.

Kirby, S. and Keay, S. (2021). *Improving Intelligence Analysis in Policing*. London, UK: Routledge.

Koper, C. S., Lum, C., and Willis, J. J. (2014). 'Optimising the Use of Technology in Policing: Results and Implications from a Multi-Site Study of the Social, Organizational, and Behavioural Aspects of Implementing Police Technologies.' *Policing: A Journal of Policy and Practice* **8**(2): 212–221.

Lambri, T., Jackson, T. and Cooke, L. (2011). 'The Challenges and Complexities of Implementing and Evaluating the Benefits of an IT System: The UK Police National Database.' In: Dawson, R. J., Ross, M., and Staples, G. (eds), Proceedings of Software Quality Management XIX: Global Quality Issues, 18–19 April 2011, Loughborough, UK, pp. 373–390. https://pdfs.semanticscholar.org/2011/35c9a9fe-9ba7aabc5ecafe4e8212d69ae54b.pdf

Lum, C., Koper, C. S., and Willis, J. (2017). 'Understanding the Limits of Technology's Impact on Police Effectiveness.' *Police Quarterly* **20**(2): 135–163.

Martin, M. and Jackson, T. (2008). *Personnel in Practice*, 4th edn. London, UK: CIPD UK.

Moore, R. (2021). Speech by SIS Chief Richard Moore: Human Intelligence in the Digital Age. https://www.sis.gov.uk/richard-moore-first-public-speech.html (accessed 13 December 2021).

National Audit Office. (2021). The National Law Enforcement Data Programme. https://www.nao.org.uk/wp-content/uploads/2021/09/The-National-Law-Enforcement-Data-Programme.pdf (accessed 28 February 2022).

National Crime Agency. (2014). *National Strategic Assessment of Serious and Organised Crime*. Warrington, UK: National Crime Agency.

Neyroud, P. and Disley, E. (2008). 'Technology and Policing: Implications for Fairness and Legitimacy.' *Policing: A Journal of Policy and Practice* **2**(2): 226–232.

NPIA. (2009). IMPACT Programme: Police National Database—Privacy Impact Assessment. http://library.college.police.uk/docs/npia/PND-Privacy-Impact-Assessment-V1.pdf (accessed 13 December 2021).

O'Neil, A. (2017). 'Australia and the "Five Eyes" Intelligence Network: The Perils of an Asymmetric Alliance.' *Australian Journal of International Affairs* **71**(5): 529–543. doi:10.1080/10357718.2017.1342763.

Olver, K. and Cockbain, E. (2021). 'Professionals' Views on Responding to County Lines-related Criminal Exploitation in the West Midlands, UK.' *Child Abuse Review* **30**(4): 347–362. doi:10.1002/car.2704.

Pinkney, L., Penhale, B., Manthorpe, J. et al. (2008). 'Voices from the Frontline: Social Work Practitioners' Perceptions of Multi-Agency Working in Adult Protection in England and Wales.' *Journal of Adult Protection* **10**(4): 12–24.

Pratt, M. (2012). *Evaluation of Interdisciplinary Collaboration in Design Research*. Unpublished MA thesis, San Jose State University. http://www.sjsu.edu/anthropology/docs/projectfolder/Pratt_Mark_project.pdf

Ratcliffe, J. (2008). *Intelligence-led Policing*. Cullompton/Devon, UK: Willan.

Ratcliffe, J. H. (2005). 'The Effectiveness of Police Intelligence Management: A New Zealand Case Study.' *Police Practice and Research* **6**(5): 435–451.

Rutgers, M. R. and van der Meer, H. (2010). 'The Origins and Restriction of Efficiency in Public Administration: Regaining Efficiency as the Core Value of Public Administration.' *Administration and Society* **42**(7): 755–779.

Sanders, C. B., Weston, C., and Schott, N. (2015). 'Police Innovations, "Secret Squirrels" and Accountability: Empirically Studying Intelligence-led Policing in Canada.' *British Journal of Criminology* **55**(4): 711–729.

Say, M. (2021). Home Office Retains CGI for Police National Database. https://www.ukauthority.com/articles/home-office-retains-cgi-for-police-national-database/ (accessed 28 February 2022).

Schwab, K. (2015). The Fourth Industrial Revolution: What It Means and How to Respond. https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution (accessed 16 February 2022).

Stanier, I. P. (2013). *Contemporary Organizational Pathologies in Police Information Sharing: New Contributions to Sheptycki's Lexicon of Intelligence in Policing*. Unpublished PhD thesis, London Metropolitan University. https://ethos.bl.uk/OrderDetails.do?uin=uk.bl.ethos.590116

Statista. (2022). Number of Police Officers in the United Kingdom in 2021, By Police Force. https://www.statista.com/statistics/877540/leading-police-forces-by-officer-numbers-in-the-uk/ (accessed 4 May 2022).

Stripe, N. (2021). Understanding the Impact of the Pandemic on Levels of Crime in England and Wales. https://blog.ons.gov.uk/2021/11/04/understanding-the-impact-of-the-pandemic-on-levels-of-crime-in-england-and-wales/ (accessed 16 February 2022).

Syed, M. (2015). *Black Box Thinking: The Surprising Truth about Success (and Why Some People Never Learn from Their Mistakes)*. London, UK: John Murray Publishers.

Taylor, R. (1990). 'Interpretation of the Correlation Coefficient: A Basic Review.' *Journal of Diagnostic Medical Sonography* **6**(1): 35–39.

Thomas, R. and Walport, T. (2008). Data Sharing Review Report. http://webarchive.nationalarchives.gov.uk/+/http:/www.justice.gov.uk/docs/data-sharing-review.pdf (accessed 13 December 2021).

Tilley, N. (2005). *Handbook of Crime Prevention and Community Safety*. London, UK: Willan.

Van Staden, L., Leahy-Harland, S. and Gottschalk, E. (2011). 'Tackling Organised Crime through a Partnership Approach at the Local Level: A Process Evaluation.' Home Office Research Report 46. London, UK: Home Office. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/116532/horr56-report.pdf

Waterhouse, J. (2019). 'Criminal Escaping Justice' Due to IT System. https://www.bbc.co.uk/news/uk-46964659 (accessed 16 February 2022).

Weisburd, D., Mastrofski, S. D., Greenspan, R., McNally, A.-M., and Willis, J. J. (2003). 'Reforming to Preserve: COMPSTAT and Strategic Problem-Solving in American Policing.' *Criminology and Public Policy* **2**(3): 421–456.

White, M. (2009). *Health, Social Care and Housing Partnership Working Briefing Notes for Practitioners and Managers*. Edinburgh, UK: Joint Improvement Team.

Wilks, L. (2014). *Break on Through: Overcoming Barriers to Integration*. London, UK: New Local Government Network (NLGN). https://www.newlocal.org.uk/wp-content/uploads/BREAK-ON-THROUGH2.pdf

Williams, J. and Britton, P. (2020). GMP have Declared a 'Critical Incident' After a Failed Upgrade of Their Troubled iOPS IT System Left Officers Recording Incidents on Paper. https://www.manchestereveningnews.co.uk/news/greater-manchester-news/gmp-iops-computer-system-error-17691657 (accessed 16 February 2022).

Willis, J., Mastrofski, S., and Weisburd, D. (2007). 'Making Sense of COMPSTAT: A Theory-based Analysis of Organizational Change in Three Police Departments.' *Law and Society Review* **41**(1): 147–187. doi:10.1111/j.1540-5893.2007.00294.x.

Wilson, R. and Gray, A. (2015). *Information Sharing: Easy to Say Harder to Do Well*. Leicestershire, UK: Centre of Excellence for Information Sharing. www.information-sharing.org.uk/download/455

Wilson, R., Martin, M., Walsh, S., and Richter, P. (2011). 'Re-Mixing Digital Economies in the Voluntary Community Sector? Governing Identity Information and Information Sharing in the Mixed Economy of Care for Children and Young People.' *Social Policy and Society* **10**(3): 379–391. doi:10.1017/S1474746411000108.