Article

Theoretical Criminology
1–21


Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/13624806251334954
journals.sagepub.com/home/tcr


‘The dream to know everything about everyone’: Affordances of commercial data systems and digital net-widening in policing

Katerina Hadjimatheou
University of Essex, UK

Pete Fussey
University of Southampton, UK

Abstract

This article empirically analyses the use of new commercial integrated data systems in policing. We examine the impact of one of the most widely used commercial systems in the United Kingdon, through observations of platform use and in-depth interviews with users across ranks and strategic, tactical and operational roles; and across specialist units including criminal intelligence, ‘county lines’ organised crime and victim safeguarding. Drawing on analytical tools science and technology studies, our analysis digitally nuances Cohen’s seminal concept of net-widening by examining how digital policing is predicated on complex police–commercial relationships. We show how the data system itself generates affordances that drive insatiable data collection, transforms mundane encounters into surveillance opportunities, revalorises mundane information as intelligence, and reconfigures the meaning of suspicion and disrupts the temporalities of policing itself. These undermine increasingly fragile principles of police legitimacy and due process, and raise concerns around transparency and accountability in policing.

Corresponding author:
Katerina Hadjimatheou, University of Essex, Colchester, UK.
Email: kdhadj@essex.ac.uk

Keywords
policing, digital, data, affordance, predictive, platform, surveillance, net-widen, police

Introduction

Recent years have seen rapid growth in the prominence and scope of 'digital criminology', reflecting broader academic, public and political interest in the impact of technology on society. This rich and diversifying field features empirical studies of police technology and digital practice, including predictive policing platforms (Brayne, 2021; Ferguson, 2017) and innovative surveillance tools, including body-worn video (Newell, 2021) and facial recognition technology (Fussey et al., 2021). This article examines the less-visible systems and practices that constitute the foundations of police data, and support, supply and sustain many of these better-examined digital tools. Drawing on findings from the first in-depth empirical examination of a police 'integrated data system', our analysis seeks to make an empirical and conceptual contribution to this emergent subfield of criminology.

The 'integrated data systems' analysed here are at once more mundane and more fundamental than the futuristic biometrics and predictive techniques prominent in the public and political imagination. Mundane because they constitute repositories of information. Foundational because they structure, store and make accessible the data required for all aspects of police work. Integrated data systems supply the intelligence logs, offending patterns and crime-recording data needed for predictive policing, real-time monitoring platforms and other cutting-edge analytics, and provide data for strategic decision-making about investigative priorities and resourcing. The article reveals the key role played by private entities in public policing. Most directly, the logics of commercial products that inform police decision-making remain inscrutable, generating obvious consequences for transparency and accountability. Yet, this analysis also traces the emergence of more complex public–private imbrications. These include how affordances of data management platforms subtly shape policing. The design and operation of such tools therefore holds enormous significance for the way police work is enacted, yet their gradual adoption throughout policing in the UK and elsewhere has received only limited scrutiny.

In this analysis, we bring Cohen's celebrated concept of 'net-widening' into dialogue with science and technology studies (STS) to digitally nuance longstanding criminological framings for the exercise of control strategies. In particular, theorisations of affordances are used to analyse how design features of integrated data systems shape contemporary police work. We argue that database integration invites new and intensified data-gathering imperatives. These in turn erode boundaries between relevant and irrelevant intelligence, policing and non-policing purposes, criminal and non-criminal, intelligence and operational domains, and actionable and non-actionable information. The effect is to destabilise long-established legal and operational constraints on the exercise of police powers to gather and act on information about members of the public. Here, we theorise these outcomes as a kind of 'digital net-widening' and make a case for the enduring value of the net-widening metaphor in contemporary technologically augmented criminal justice practices.

Net-widening in the digital age

Stanley Cohen's (1985) metaphor of net-widening advanced Foucault's highly influential analyses of the microgeneration of control. The concept has been applied widely since, and has enduring value in identifying problematic coercive 'creep', where 'more and more individuals become subject to the scrutiny and surveillance of criminal justice personnel' (Lowman et al., 1987: 211). The effects, if not the label, of net-widening in police surveillance, use of force and social control have been discussed in relation to predictive policing, tasers and electronic monitoring (respectively Brayne, 2021; Byrne and Marx, 2011; and Nellis et al., 2013). Others have emphasised the encroachment of policing into the civic realm, for example, on the 'criminalisation of social policy' (Rutherford, 2000), whereby social 'problems' become increasingly recast as matters of law and order, meriting an enforcement and punitive response, with discussions around 'anti-social behaviour' being one totemic area of debate.

While the concept of 'net-widening' has become part of the criminological vernacular and a shorthand verb for coercive overreach, it has lost much of its complexity. Re-examining net-widening in the context of digital policing reveals enduring relevance in several original features of Cohen's argument. Like Foucault, Cohen focuses on 'punishment and classification' (1985: 4), although he places heightened emphasis on the additive, rather than substitutive, role of micro-level articulations of power. Put simply, measures introduced as alternatives to custody became additions to custody. At its most fundamental level, Cohen's thesis alerts us to three vital considerations that resonate with this analysis of digital policing: the forms, processes and drivers of coercive expansion. Each is discussed in turn.

Forms of coercive expansion have attracted the most familiar application of the net-widening idea. Here, for example, 'alternatives [to custody] have left us with wider, stronger and different nets' (Cohen, 1985: 38). Three elements of coercive expansion are pertinent for analysing control in the digital age: quantity (the scope and reach of coercive expansion); identity (the visibility of processes); and 'the ripple problem' or the knock-on effect. This article explores the durability of these ideas in the digital context through manifestations of creep, surveillance asymmetries and collateral intrusion.

Regarding 'processes', Cohen situates monitoring and surveillance as not just an objective, but also the mode of knowledge production: 'surveillance, not just punishment, became the object of the exercise' (1985: 26). Such insights help reveal how the technologies examined in this article are more than mere additions to the repertoire of control measures; they shape the modalities of seeing, knowing and 'doing' more generally. This theme also resonates with how technology becomes implicated in knowledge production. Relevant here are Lyotard's (1984) critique of how 'knowledge' becomes reduced into selective forms of computer-generated 'information', and how predictive data is enmeshed in complex regimes of digital power/knowledge (Aradau and Blanke, 2017).

Although the drivers of coercive expansion lie outside the scope of this article, Cohen's analysis is instructive for considering adjacent concerns. Political economy is one obvious site of analysis for examining expanding control mechanisms. Here, the management of new criminal categories provides opportunities for market expansion. Cohen reserves caustic analysis for prominent intellectual framings that neatly cleave

the world into simple binaries of state and corporate interests or, alternatively, claim symmetrical interests between them. While commercial opportunities arise through the privatised management of deviant bodies, capital responds to crisis in complex ways. For example, Cohen correctly identified how a move away from the state went beyond reliance on private capital, and enabled diverse regimes of knowledge as part of the increasing dominance of professionals in justice practice. By extension, the diversification and extension of control brought an expanded range of legal, quasi-legal, discretionary, administrative and professional expertise, where 'each set of experts produces its own scientific knowledge' (1985: 86). Thus, in the context of advanced digital policing tools, private knowledge becomes implicated though intricate modalities. These include the commercial design choices encoded into proprietary algorithms or the structuring of data to make it legible for officers and invite specific policing actions.

Crucial to this article is Cohen's designation of 'the system' as something dynamic and kinetic, growing and reshaping through the practice of control. Control mechanisms are seen not as fully formed at conception, but as acquiring shape, status and influence through practice. Resonating with later theorisations of socio-technical assemblage (see below), such observations owe a debt to Heidegger's (1962) foundational work on 'being', and its emphases on how substance and meaning arise through action. Ramifications for empirical enquiry include the importance of interpreting the tools and practices of control in their operational context. In the digital era, this insight further highlights the importance of examining how human and technical elements interact, shape each other and assert specific net-widening outcomes, through policing.

The expanding uses of novel digital tools by law enforcement invite an examination of the intersection between Cohen's framing and the growing entanglement of humans and technology investigated by STS. Notable milestones in this conceptual territory include the social construction of technology (SCOT) perspective that emphasised the social, political and cultural shapers of technology (inter alia Bijker et al., 1987). SCOT's fundamental contribution is its challenge to technological determinism via its emphasis on how technology is shaped by the social settings in which it is deployed. This approach has since been supplanted by other perspectives including actor network theory (Latour, 2005), which criticises the ontological separation of humans and non-human objects, and its perceived overemphasis on human agency. Put simply, it addresses both how technological outcomes become shaped by their context and how technologies shape their environments. A key intervention in this debate emphasises the performative character of such interactions, where outcomes occur through practice, such as the 'constitutive intertwining exist[ing] between material and human agency' identified by Pickering (1995: 15). In this account, 'machines' are 'enveloped by human practices' and 'constitutively intertwined'. Human agency exists yet becomes calibrated to its material environment; less of a mutual shaping than a mutual accommodation between human and non-human elements.

With respect to surveillance and other policing technologies, these ideas resonate strongly with concepts of assemblage and emergence as elaborated by Deleuze and Guattari (1987) and others. One key concern in this literature is the emergence of new practices and outcomes arising from the union of human, technological and environmental phenomena. More recent still are attempts to theorise human–non-human

(technological) imbrications through the lens of 'new materialism' (Lemke, 2021). These accounts include effort to reclaim Foucauldian thought, such as Lemke's (2021) adaption of Foucault's (2007) concepts of 'dispositif', 'technology' and milieu. Another approach invokes quantum physics, notably thought the recent advancement of 'entanglement theory' (Wendt, 2015) to consider the relevance of sub-atomic particle interconnectedness to the social world.

Drawing these theoretical strands together, analyses of human and non-human meshing provide rich new conceptual vocabularies to address the dualism between technologies and the social and to re-examine Cohen's thesis in the digital age. In particular, this article argues that bringing criminological ideas of net-widening into dialogue with STS emphasises and develops important nuance in Cohen's original work. For example, many applications of net-widening consider it an effect (or effects) of novel control sanctions. Retaining fidelity to the original idea, we explore the dynamics of net-widening as a foundational process arising through the practice of digitally mediated policing.

To achieve this, the article operationalises the STS concept of affordances. Affordances refer to the interplay of the technological and the social to consider how objects invite (rather than determine) certain actions (Hutchby, 2001). As Fussey and Roth (2020: 663) note, affordances define the 'possibilities that *enable and constrain action*'. In doing so, space is created for policing discretion and subjectivities to remain relevant. In a further adaptation, while studies of net-widening tend to emphasise impacts on 'suspects', this article analyses how net-widening 'affordances' introduced by integrated data systems generate future expansionary possibilities. Furthermore, extending beyond the traditional focus on justice agencies, strategists and policymakers as the principal agents of net-widening, we explore the role of police and the technology developers who together co-produce those systems. Highlighting the role of these actors is vital to understanding the dynamics of control and, ultimately, accountability over the structure and contours of digital policing.

The article begins by examining the accelerating process of digital transformation in policing, setting out the context in which the commercial integrated data system examined here – known as 'Athena' – has been developed and implemented in the United Kingdom (UK). We then outline the methodological approach before presenting the data over three areas of analysis. The first reveals the complexity and digital nuancing of commercial–technical policing relationships. These, in turn, impact the nature and temporality of digital policing practices, analysed respectively in the second and third data sections. We conclude by examining the implications for net-widening theory, and the future research agenda of digital criminology.

Data integration and digital transformation in policing

At the time of writing, UK policing is undergoing a period of intensive 'digital transformation', marked by several initiatives. One common ambition is the consolidation of previously standalone databases (for intelligence, cases, custody records and other information) into single integrated systems, supplied by commercial technology providers. This trend towards data integration reflects a growing consensus in policing that easier access, search, analysis and sharing of all police information are essential to

basic efficiency and a prerequisite to many of the digital innovations on the professed 'transformation agenda' (Association of Chief Police Officers [ACPO], 2020). Relevant innovations include bulk intelligence analysis, big data applications, and predictive analytics.

Between 2005 and 2019, nearly all police forces in England and Wales purchased or developed an integrated data system. Integrated systems are cloud-based web services that merge myriad police functions into a single platform, including intelligence, investigations, case management and custody data. Such platforms offer a single digital entry point for officers accessing computers or mobile devices, and a unified system through which to build, track and manage a case; log intelligence; input incidents; generate warrants; and so on, without having to re-key information manually. Integrated systems ideally offer three capabilities: they support real-time analysis of operational information, intelligence and performance; link police forces enabling more efficient data sharing; and integrate existing data such as automatic number plate recognition or body-worn video footage. The breadth of such platforms signals the extent of police digitisation and the growing importance of considering human–technology relationships in this context. The cost of purchasing and maintaining integrated systems varies widely but collectively constitute the 'largest investment in police technology in a decade' (NEC, 2022). London's Metropolitan Police Service, one of the largest in the world, is predicted to spend £214 m on the purchase and maintenance of their system over a period of 10 years.

Despite this significant investment, a 2018 survey of police attitudes to information technologies (IT) revealed that only 2% of police officers were satisfied with their IT systems, and only 30% thought their force invested wisely in them (CoPaCC, 2018). The UK media reported several scandals and failures between 2009 and 2022 (Hadjimatheou, 2021), documenting frequent system crashes, failures to record hundreds of thousands of crimes of abuse (including child abuse), inadvertent publication of sensitive information about victims, and erroneously recorded information leading to wrongful arrests (Hadjimatheou, 2021). In one regional police force , problems resulted in the resignation of the chief constable and scrapping of the multimillion pound commercially provided system. Despite the design and, in some cases, active operation of these systems by private companies, there has been no discernible effort by appropriate oversight bodies to hold them accountable for their role in police failures. Contractual agreements remain shielded by commercial confidentiality. At the time of writing, we are aware of no academic research examining the impact of this new generation of commercially provided integrated data systems on UK policing. This article aims to address this lacuna.

Athena

This article focuses on the implementation of an integrated data system, Athena, shared across nine police forces. Athena is an 'integrated' system in two senses. First, and most directly, Athena connects data across each stage of an investigation, from an incident recorded on a mobile police device, to the eventual court process. It encompasses intelligence, investigations, custody and cases. Second, Athena connects and makes visible data to any officer logging into the platform from nine different police forces for any

operational reason. They can navigate between functions and search for specific individuals, addresses, and information about persons and places across each area.

Athena also incorporates analytical tools developed or purchased by forces for additional functions, such as automatically generating a monthly risk ranking for domestic abuse victims and a weekly assessment of gang activity and suspected protagonists in a specific region. Athena provides push notifications and allocates tasks so that officers logging in can keep up to date with their work and track progress. It also logs all officer activity, enabling anti-corruption monitoring and investigation. Finally, Athena serves as a source of longitudinal data for research and analysis for the police and their partners.

Athena's basic operating system, Connect, is the most widely adopted integrated system in UK policing. Supplied by Northgate, an acquisition of Japanese technology giant NEC, the 'Connect' platform is currently used by 16 (of 43) UK constabularies including the two largest metropolitan policing forces, making it the market leader by a significant margin (NEC, 2021). By design, Northgate's systems are interoperable with NEC's significant range of security technologies for the public sector, including artificial intelligence and biometric tools such as facial recognition technology. In terms of contractual obligations, Northgate's police clients typically subscribe to the Connect system for an initial period of 10 years.

Connect subscribers pay a higher fee for independent standalone servers that allow control over the management and development of the system. Athena subscribers, all of whom are locked into contractual arrangements until at least 2029, negotiate collectively for changes and improvements via a decision-making body known as the Athena Management Board.[1] This board represents an additional, and opaque, layer of police–commercial relationships, comprising seconded representatives from consortium forces and Northgate. Seconded force representatives include a chief inspector and 'business adviser experts' who represent force interests and propose system adaptations in areas such as intelligence handling, case management and custody records. As elaborated through the data below, Northgate retains significant financial leverage in these negotiations, yet the nature and content of these discussions are hidden from public scrutiny and accountability.

Methodology

We conducted interviews and observations with police officers and staff working for Force A over six months during 2019–2020. Force A was one of the first to implement data integration across its work areas and to procure an integrated data system. Force A also has a professional reputation for being at the forefront of data analytics in policing nationally. At the time of data collection, Force A was undergoing significant organisational changes driven by digital transformation of everyday police work. This involved substantial investment in data scientists, training and technologies, reorganisation of data architecture and digitised performance monitoring across the force, and a new data-sharing partnership with local government, social services and academia. Access to participants was granted at a senior level by Force A, and researchers made contact directly with individuals by email referencing their authorisation by chief officers.

The main research aim, co-produced with Force A, focused on data use, demand and challenges across police forces, especially in light of the recent push to become more 'data driven'. Because very little was known about police officers' own perceptions, experiences and operational engagement with such technology, we adopted what Hunter et al. (2019) call a 'descriptive–explorative qualitative approach' to interrogate new practices that have previously received little or no systematic attention. Questions examined participants' engagement with different kinds of data and technologies, explored how they leverage the actual and potential value of data, and addressed perceived limitations and challenges of existing digital products through the course of their policing practice. Researchers were given frequent demonstrations of aspects of the system's functionality, structure, snags and constraints, so police could 'show' as well as describe the issues they discussed.

Participants were diverse, representing all ranks and relevant departments including the 'Athena team', criminal intelligence, strategic change, data analysis, domestic abuse, serious crime directorate and other specialist teams including gangs, drugs, 'county lines'[2] and victim safeguarding. Participants occupied strategic, tactical and operational roles. Eight participants held a specialist data analysis or technology-related role. Eleven were frontline officers. About one-third of participants had some experience of 'legacy' force data systems; existing systems that became 'integrated' into a single solution by the Athena project. This latter group of participants provided valuable insights into both the differences between Athena and the 'legacy' systems, and the impact on police work of the introduction of the former. In terms of demographics, there were 24 men and 21 women, and all bar one were white British, reflecting local demographics.

Data was interrogated through a combination of thematic and narrative analysis with information managed through NVivo software. Thematic analysis revealed common aspects and outcomes of data and system use across the diverse roles and ranks of our participants. A narrative interpretation facilitated assessment of the meanings attributed by officers to their force's investment in, and strategic use of, data, and their engagement with different actors, environments and forms of technology. This dual strategy facilitated a nuanced analysis, capturing both the overarching patterns and the unique, contextualised interpretations of participants. Together, these approaches assist a rich and multidimensional examination of the findings.

Snags and entanglements: Private knowledge and public policing

The relationship between the 'public' police and commercial actors providing 'policing' roles has been a rich area of criminological enquiry (inter alia Button, 2019), which considers such unions in relation to neo-liberal forms of governance (Lacey, 2013), corporate logics and power–knowledge arrangements (e.g. governmentality; Foucault 2007). This first data section expands on that existing literature to reveal how the operation and management of Athena suggests a more complex and digitally nuanced relationship between commercial–technical knowledge and the exercise of public policing.

Under the police–Athena contract, the technology developer assumes responsibility for construction of the system and its ongoing maintenance. This raises fundamental questions over system and data ownership, liabilities, maintenance and the resolution

of data snags and entanglements. With whom does accountability lie when the system ruptures or fails? Here, we examine the problematic ways in which control is exerted by the technology developer over those affordances and constraints of a system that shapes police practice.

Police in Force A cannot correct, update or improve any aspect of Athena themselves. Instead, they rely on Northgate for even minor changes, which require negotiation with both the developer and other consortium forces through the Athena Management Board. Although the board operates in secrecy, limiting the accountability of policing decisions, participants expressed the laborious, fractious and unsatisfactory process for improving the platform. Proprietary arrangements introduce rigidities and fixity into the system, thus undermining Northgate's claims to deliver 'agile' commercial solutions. This inability to refine the system prevents police from fulfilling legal duties to safeguard those in situations of vulnerability. For example, one domestic abuse safeguarding expert explained how the design of input fields in Athena prevented properly recording and linking a child to a case or incident, despite this being a legal obligation, and that any refinements required a laborious process,

> … the problem was that whatever changes we want to try and make on Athena, they have to go through all the other forces for them to agree and then they've got to try and work out how they do it. (Police domestic abuse safeguarding lead)

A senior intelligence officer raises another manifestation of rigidity, describing an inability to remove an unhelpful experimental tool he designed within Athena due to costs requested from Northgate. He explained how the tool continues to generate useless weekly rankings of high-risk suspected domestic abuse victims, which complicates the prioritisation of cases for officers working with victims. These officers receiving outputs from this tool confirmed its fallibility, with one explaining, 'it's identifying the wrong people… victims have appeared on there that shouldn't, and victims who should appear on there haven't'. The affordances of this technology intersect with organisational distributions of liability and blame. When asked why they use it, another safeguarding officer said they felt obliged to rely on the ranking because to ignore risk that is officially flagged by a data system would expose them to disciplinary measures, 'If someone then died on that matrix and we've ignored it, then we're open for criticism'.

Additional frustrations over the dysfunctional elements of Athena existed across the ranks. For example, one senior officer similarly expressed frustration with Northgate not 'delivering what was promised' and a disempowerment in the face of 'great costs' charged by the company to address faults. One senior officer directly involved in negotiations with Northgate highlighted further disparities in this relationship,

> Officer: Where there's something we would like to be different, we then pay for the privilege of the change.
>
> Researcher: Are the requested changes value for money?

> Officer: I'm struggling even with a political answer on that one. Many would say the prices are extortionate… if the [consortium] forces say, 'this change is a priority,' and Northgate price it and give us back an impact assessment which says it will cost £100,000 to make this change. Our IT [department] cannot go into the system to review it, to assess whether or not they consider that's value for money or not. We're dependent on the honesty of Northgate. Do I think all the changes are value for money? [Smiles] You can decide.

Data integration therefore entails myriad hidden financial, agential and accountability costs. The asymmetry of police–corporate relationships is also extended by such arrangements. Crucially, the vulnerable people such systems purport to serve are also left with fewer protections. These dynamics also undermine the corporate narrative that commercial and technological processes are more efficient and effective. The following sections demonstrate how actual operational uses of Athena assert further influences on the scope and temporality of digital policing practices.

Widening, thinning and linking the net(s)

'We're trying to fill it all up.' Thinning the mesh through data granularity

Northgate's marketing materials about Athena feature its ability to store and structure a 'rich dataset' and offer 'instant access to all the information we have about a potential suspect' (NEC, n.d.). Few limits constrain Athena's storage capacity. One senior intelligence analyst explained how Athena's net-widening potential promises to achieve the (illegal) 'dream' of policing:

> … the dream world as far as policing goes is to know everything. That's always the dream: to know everything about everyone. But, obviously, that is completely unrealistic … what everyone is working towards is a forum where, when we identify someone [of interest] we can identify all the information available about that person…. The dream is that we can go, 'Right … we know everything that everyone has on these people right now'.

To achieve this dream, frontline officers described how they take advantage of each public encounter to collect increasing volumes of data. As one officer explained, the pursuit of this exerts the added implication of eroding any boundaries between 'criminal' and 'non-criminal' information,

> It's like we're trying to fill it all up, get as much information as we can about everyone.… (Frontline officer)

Another participant explains how the shift from old systems to Athena invites the recording of far more detailed information than previously. This includes granular descriptions of incidents and their protagonists:

> … everything, custody, intelligence, warrants, searches, everything goes onto Athena…. You can definitely see a trend, if you go back to some of the earliest records, the data we actually have is quite minimal. When someone was arrested for a crime in 1980, on [the 'Police

> National Computer'], for example, it will just be recorded as the very facts of the robbery – entered address as trespasser, stole things – and it will be nothing. Now we put quite a detailed; how they got in, tools used, damage caused, full extent of all rooms…. So, we're improving the quality of the data, the volume of the data perhaps, and far more descriptive. (Detective)

More people are also included in the pool of police data, because any contact with the criminal justice system is now captured and classified in a coherent record on the platform:

> … if you've ever been a victim, a suspect or witness to a crime, you'll be on the system. If you've ever acted as an appropriate adult for somebody in custody … If there's someone you know in custody and they've phoned you from custody, your name and contact number will be in there [and] probably an address. And a date of birth. But if you've been a suspect, so a photo, fingerprints, DNA, all that sort of stuff. All your previous [offences] – whether it went to court, whether it didn't. Doesn't matter. (Frontline officer)

The demand for ever more detailed data collection is expressed by one detective as genuinely insatiable:

> Researcher: Do you think, is there ever too much data?
>
> Detective: Too much data? No. I encourage my colleagues to do more, always put more on.

Prior to Athena, officers would input data into separate databases devoted to a specific crime type or policing function. Athena's integrated structure and infinite storage capacity designs multiple uses into the fabric of the system. This enables data gathering to become decoupled from specific purposes, subjects and objects. Here, there is no expansion in surveillance purposes or 'surveillance creep' (Marx, 2002). Instead, interoperability is encoded from the start. As one detective sergeant explains, in an account that conflicts with data protection law's insistence on defining the purpose of processing in advance of its implementation:

> … if you're obtaining the data and you're obtaining that lawfully, why would you then not use it for other areas of business? We can store large amounts of data now, so what's the issue? (Detective sergeant)

In this sense, Athena offers affordances that invite an expansion of police data-gathering practices. Athena's integration of intelligence, operational, administrative and public protection functions ensures it becomes a repository for increasingly diverse categories of data. Also notable was the commonly expressed 'if Amazon can collect data why can't the police' argument, one that is selective in its appreciation of both the law and the monopolies of coercive force invested in democratic policing structures.

Nowhere is the rapacious collection of information more evident than in the loosely defined category of 'intelligence', which participants consistently deployed to justify their data-gathering practices. As one senior detective stated,

> … our actual intelligence – 'so-and-so was seen walking down the street in company with another person'… – all that data should get recorded on the system and I encourage my colleagues to put more on because the amount of times I've searched for something and, at the time, the person didn't know its relevance, but six months down the line … becomes part of my investigation.

To continue Cohen's metaphor, Athena 'thins the mesh' by capturing finer detail on individuals and their associations. Here, broad aims of situational awareness (understanding the environment and being ready to respond) and unbounded categories of 'intelligence' justify speculative and insatiable data-gathering practices. Athena's accommodation of such data generates an affordance that invites the collection of more mundane information, which, through storage on this digital platform, becomes classed as intelligence even if entirely irrelevant to an offence:

> And we come across things, you know, just things that police should be aware of that we're always gathering, always making a note. (Detective)

In this regard, Athena allows police activities to be refocused in ways that extend the horizons of police intelligence-gathering activities. Athena allows 'data' and 'intelligence' to become synonymised, where the former refers to any and all information and the latter normally refers only to information that serves a crime-preventive purpose. This participant further explained how such platforms not only provide additional surveillance capability, but they also offer extra-procedural tactics in unregulated areas of practice. For example, these tools convolute the (already indistinct) distinction between covert and overt policing:

> They are undertaking sort of covert work, I suppose…. They're out there undercover but seeing what people are up to in the widest sense…. Taking that little snippet of information and developing it through to the point at which you can action via whatever means, whether it be getting [a subject of interest] stopped in the street, getting their car turned over, obtaining a warrant for the address. (Intelligence lead)

As the scope of data gathering broadens, its role within policing shifts, and its specificity of purpose depletes. The above accounts of how data gathering becomes pursued in operational settings reveals a decoupling of data collection from specific purposes. This is pursued with the unlimited aim of cultivating 'situational awareness', which also establishes grounds for future suspicion.

Research on digital police platforms has recognised similar processes of heightened information gathering, such as Brayne's (2021) concept of 'dragnet surveillance'. Yet the data here also reveals an epistemic shift, one marking subtle but fundamental changes in how suspicion is formulated. Additional to using surveillance and intelligence to confirm a suspicion, investigations emerge from speculatively acquired intelligence. The abundance and accessibility of data allows case-building to become more inductive than deductive. A balance shifts. This marks a form of 'surveillance without looking' that coexists with more traditional forms of directed surveillance. Longstanding distinctions

in policing, such as directed versus non-directed surveillance, and basic governing thresholds such as 'reasonable suspicion' are all challenged by these activities.[3]

Strengthening the net: 'Some people won't realise they're telling us things that they otherwise shouldn't'

Supplementing the increased breadth and granularity of information, intelligence capability becomes further enhanced through the heightened connectivity and visibility of data. This 'net strengthening' is delivered through technical and organisational means. Taking these in turn, Athena's digital architecture facilitates linkages between disparate information sources. Distributed information becomes meshed in new ways, allowing non-obvious associations to surface. Although this may suggest a straightforward element of data management, the level of data richness and integration is unprecedented.

Cohen (1985) observed that one net-widening mechanism involves the merger of previous distinctions between categories of persons, such as offender/suspect, vulnerable/dangerous. Such unions widen the definition of who becomes designated as a legitimate subject of state control and surveillance. Developing this insight in the context of digital policing, the data-gathering imperative exerted by Athena alters the nature and objectives of police–public interaction, specifically by encouraging officers to reconstrue citizens as sources and police–citizen encounters as intelligence-gathering opportunities. As the following account from a senior intelligence officer shows, Athena creates affordances that reframe and blur the boundaries between crime-reporting members of the public and police informants,

> Those contacts could be a neighbour that might, in the future be of use … So, 'could you maintain a relationship with such-and-such and give us information about them … or keep an eye on this location and report when you see this, this and this going on?' Any officer has access to this system … and can equally put information onto that system. So, everything goes into that one repository for intelligence. (Senior intelligence officer)

Here, we can also see a parallel blurring between the roles of community policing and intelligence-gathering functions, thus merging collaborative and coercive policing roles in ways that may exacerbate potential tensions between them. Such activities also flourish in a context of broad police discretion offered under common law powers.

The following quote illustrates another dimension, where the intelligence-gathering imperative conflicts with the community policing aim of building trusting and supportive relationships with vulnerable citizens:

> I was driving a chap home yesterday. He was arrested for burglary, we made enquiries to prove he didn't do it. He's a heroin addict, he's now homeless, and so I was just asking him questions … where he's living, how much heroin does he take per day, who he's associated with, whether or not he's on any kind of methadone programmes, so he can get his legal substitute…. And he tells me how much he does, where he gets it, how he gets it, he's trying to cut back but it's very difficult. We have this very honest conversation about his lifestyle, but all the time I'm thinking, 'well, I'm going to have to record this' … I'm investigating a future crime. And we do that all

> the time…. Some people won't realise they're telling us things that they otherwise shouldn't. (Detective)

This encounter reveals how the officer's role takes on a duplicitous aspect, between support and surveillance that goes beyond specific individuals and fields of police enquiry: the integration of intelligence and community policing functions starts to pervade all frontline police work via the platform. As Ferguson (2017) argued in his study of predictive policing, such encounters encourage police to treat citizens as potential intelligence sources rather than citizens with rights and needs.

A variation on this dynamic arises through Athena's merging of administrative and operational functions. In one case, a safeguarding coordinator described how confidential details of violence shared by high-risk domestic abuse victims with their case workers in safety planning meetings are entered into Athena, and fully visible to other police, without the victim's knowledge or consent. This undermines professional principles of trust and confidentiality and risks that police will act on data they were never entitled to have.

Organisationally, Athena further erodes boundaries between police and non-police intelligence. In a digital reiteration of their 'knowledge brokering' role (Ericson, 1994), police distribute intelligence to myriad other parties and in turn integrate information before translating it into 'intelligence'. Here, we can see how Athena invites further net-widening by blending two functions of policework, the administrative and operational, and merges their respective forms of data. These activities practices also exist outside procedural oversight that regulate policework.

Temporalities of digital net-widening

The rich scholarship on net-widening has provided crucial insights into the expansion of coercive measures across the social body. However, as Flyverbom has noted, we still lack 'a more analytical and critical approach to the study of data analysis platforms … sensitive to implicit understandings and strategic framings of temporality' (2024: 3273). This section interrogates how Athena and similar digital policing tools generate new possibilities for expanding temporal frames of policing into the past, through the present and into the future.

Shaping the present through data currency

In the present, Athena's combination of increased volumes and immediate availability of data bolsters intelligence and situational awareness, surfaces previously obscured relationships, and helps determine the allocation of non-criminal justice resources in real time. As one intelligence officer explained, '[t]he aim of Athena is a one-stop-shop for the "golden nominal"', that is, the immediate linking and listing of formerly disaggregated information about a person, which is then made available at the click of a button. While this may seem a straightforward element of data management, the fact that, in the words of one detective sergeant, 'with Athena there's so much more information available to you much quicker', suggested a level of data richness and immediacy

that is unprecedented. The insight provided by the new system is further described by an inspector below:

> Researcher: And the PNC and the PND [respectively, national police conviction and intelligence databases] together wouldn't give you the picture?
>
> Wouldn't give you the full picture, … because [with Athena] you've got every bit of information… you're going to have the suspect details, you're going to have the victim details, you're going to have associates' of the victim's details, … you're going to have cars, you're going to have phones. You wouldn't have all of that on any other system. (Inspector, intelligence)

Athena's comprehensive but geographically localised focus offers greater data currency for 'knowing who's where and what they're doing' (frontline officer) than other police databases. This holds utility for police seeking to build rapid intelligence pictures:

> … the two biggest advantages are being able to track people and their behaviour, and all their linked activities and information and the fact that you have got an integrated process that will take you from the beginning of the investigation through to the end…. In the past, we would have had so many computer systems or have to wait for a conversation with another force…. We can click a button now. (Senior intelligence officer)

In another articulation of temporal compression, one officer explained that, formerly, those 'conversations' could take a week or more (intelligence analyst). Another said national systems were ill-paced to police fast-moving worlds of organised crime because some forces took 'months' to update the national systems, which they described as 'an eternity' in terms of crime.

Multiple officers found Athena to be more current and effective in developing tools for organised crime investigations, such as risk matrices, which prioritise the monitoring of suspected offenders and their associates. One intelligence officer explained how information on potential suspects entered into the 'matrix' elevates their risk profile, generating a recommendation to accumulate further intelligence material that is re-imported into the system, in turn increasing an individual's risk score, 'and it just goes round and round'. Such 'feedback loops' intensify the surveillance gaze (and 'thin the mesh'), and have been identified in other areas of digital law enforcement practice, such as predictive policing (Hadjimatheou and Nathan, 2022). They exemplify how individuals' exposure to police enforcement action is shaped by the affordance of their digital visibility in police data systems.

Information entered into Athena is not subject to due process, review or rectification, revealing a further dimension to such feedback loops. Here, the structuring and classification of data is subject to arbitrary processing and value-laden classifications before it becomes visible to officers. Once widened and thinned, the net thus becomes reinforced. Notable here are the high-stakes consequences for those implicated in such discretionary practices. Regardless of reasonable suspicion, being enrolled into Athena's database also offers a pretext for police intervention. For example, one organised crime detective described how they target people but 'try to make it look like a routine stop check'

where in fact they were 'looking for an excuse …to search your car for drugs, or at least to get eye to eye contact with you to see if I have got grounds to then search you under a different power'. Such accounts are analogous with controversial US police practices of discriminatory 'pretext stops' (Alexander, 2012) and 'parallel construction', in which data on Athena is used to target an individual despite insufficient grounds to do so.

Trawling for the future: From prediction to possibility

The practice and possibility of predictive policing in particular has recently become a core preoccupation of digital criminology (inter alia Brayne, 2021). Accordingly, a distinct emerging body of work examines the role of prediction – understood both as an aspiration and as an approach to policing – in shaping police data practices more broadly (Egbert and Leese, 2021). Although some dynamics and transformations are identified in relation to the introduction of predictive policing (e.g. insatiable data gathering, unlimited searchability and a focus on real-time insights) and also emerged in our analysis, prediction was curiously and conspicuously absent from many participants' accounts. Even participants whose role was devoted exclusively to data analysis did not mention prediction until prompted, and even then, responses were sceptical at best. As one data analyst said, 'we'd love to do more work on predictive policing', but doubted that 'the data that goes into the machine is of a high [enough] quality'. Another senior data specialist blamed the limited capabilities for sophisticated analysis on the 'ill-conceived, ill-thought-through' contract with the software developer who, in their words 'took advantage of everything that they could' to deliver a system incapable of extracting data for bulk analysis. One data manager further illustrated how contingent future capabilities relied on the private developer, explaining that ambitions for advanced analytics were dependent on the success of an ongoing project to enable bulk data extraction from Athena which, in his words 'should work, in theory, if it is all delivered as promised [laughs]. Yeah there's been an issue with Northgate, which runs Athena.'

Although our participants did express a preoccupation with the future, they highlighted a further dimension to the prediction-driven 'orientations towards the future' emphasised in other research (Aradau and Blanke, 2017). Here, participants emphasised a turn from prediction towards broader notions of potential, by which we mean an intrinsic capacity or latent tendency within the data to one day translate into something meaningful (e.g. intelligence categorised as relevant) or towards an outcome (a detection or prosecution). In terms of net-widening, such practices broaden the range of candidates available for scrutiny and extend the temporal window for doing so. For example, a senior intelligence officer explained that even if intelligence gathered today is never 'actioned', it 'still sits there open to all' on the system because it 'may become of use later on'. The same officer asserted that in his view 'intelligence is never necessarily going to be "irrelevant"'. This corresponds with the detective who described 'investigating a future crime' above. Indeed, the view that 'relevance' was not a requirement to justify surveillance was commonly expressed. As the following officer explains, the prospect of ex post relevance is considered justification alone. Even if a suspicion is revealed as unfounded in the moment, it may become vindicated in the future:

> … if I'm stopping someone because I think they may have drugs on them, even if they haven't, there would be a reason why I *think* they have … so that information is worth keeping … you still need it because you may end up using it at some point. (Frontline officer)

This problematic (and circular) reasoning evokes François Ewald's (2002) discussion of the 'precautionary principle': an anticipatory logic that gives weight to abductive suspicions as a justification for taking measures to prevent or avert as-yet-unknown future threats. Prediction clearly remains an aspiration for Force A, but, as Valverde (2010: 11) has argued in the context of security, 'an increase in the popularity or breach of one logic does not necessarily bring about a decline in another'. Indeed, one major contribution of Cohen's (1985) explication of the net-widening metaphor was to articulate the co-existence, and hence extension, rather than replacement, of different coercive regimes. In the context of Athena, logics of prediction, possibility and precaution co-exist. These transcend standard approaches to calculations of risk and demonstrate the multiple modalities of future-orientated digital policing.

The enduring past and digitised deviancy amplification

A distinctive affordance brought by Athena is the way it invests data with durability and longevity, allowing information to be retained over an entire lifetime,

> You can search for John Smith here [showing screen] and then you'd have every case that John Smith had been in, every investigation, every intelligence report, every person who he'd been linked to and every address that he'd been linked to and every communication device he'd been linked to. (Detective)

Unless the information is demonstrated to be false or in breach of police conduct rules, no process exists for 'filtering' or deleting police data on Athena. Instead, the meshing together of all crimes, associations, victimisations and so on, combined with the absence of a filter, means any search for a specific name reveals all linked data as far back as the records extend, leading some names to yield '1500 hits … crashing the system when you loaded them because … they had so many reports' (detective). Intelligence is, as one officer explained, 'not bound by' rules around data retention, allowing it to be kept 'forever'. These new logics of precaution and potential combine with technical affordances that invite first the collection of information and then its translation into intelligence. This in turn subverts the legal principles designed to limit the processing of personal information to what is necessary for specific policing aims. Moreover, the immortalisation of the data in Athena and its perpetual linkage with a person raises important questions around people's rights to move on from their offending histories, and legal 'rights to be forgotten' and 'rights to erasure'.

Conclusion

Our analysis reaffirms the enduring value of the net-widening metaphor in criminal justice, while also demonstrating how the process and practices surrounding integrated data systems nuance the concept, and the key role played by private actors and entities.

At a time when declining trust and confidence in policing is of acute public concern, questions over relationships between commercial technology providers and public policing, and their impact on transparency and democratic accountability are urgent and perhaps more pressing than ever before. We have shown how the relationship with this private tech developer, variously described by participants as unequal and extortionate, entails arbitrary contractual commitments and privileges technological affordances, which in turn shape the capabilities and outcomes of police data systems. Yet, at the same time, the capabilities offered by commercial actors, combined with regional market capture, make those contracts irresistible, exerting a driving force on police technology developments that is both pivotal and largely hidden from public and democratic scrutiny.

These digital capabilities are significant. Athena's ability to link intelligence data and increase the visibility of finer-grained information constitutes a 'digital net-widened' intensification of surveillance capability. Existing policing processes become extended and intensified (respectively, a widening the net and thinning the mesh). At the same time, Athena invites shifts in policing practice, including the deeper integration of operational and administrative tasks. These culminate in the emergence of genuinely transformative outcomes. To extend the metaphor, beyond adding scale and granularity to nets, as traditionally conceived, is the issue of connectivity by linking data edges and databases (the joining of different 'nets'). Further, Athena brings changes to the temporalities of data-driven policing data in ways that suggest new directions for analysing police engagement with predictive analytics. Supplementing 'the belief that the accumulation of sufficiently large amounts of data would render the world, if not better understandable, at least better predictable' (Kaufmann et al., 2019: 677), we see instead that such data handling practices bring epistemic shifts in digital policing.

For Foucault (2004), power was productive, something exercised rather than hoarded. Much Foucauldian (and post-Foucauldian) theorising on control has emphasised the goal, indeed aspired apotheosis, of efficiency as one key element animating such exercises of power. Indeed, promises of efficiency are central to the hype that accompanies digital policing tools such as Athena. Yet our findings suggest that operational uses of Athena pursue different priorities. Efficiency –and, as the data reveals, accuracy– becomes relegated below another aim: accumulation. Paradoxically, 'efficiency' in the context of Athena entails collecting everything, forever. Athena invites police to treat all 'information' as potential 'intelligence' and, in so doing, affords data durability via the prospect of future value. This in turn offers the promise of Athena: 'the dream to know everything about everyone'.

Declaration of conflicting interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The authors disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the Economic and Social Research Council, (grant number ES/ M010236/1).

ORCID iD

Katerina Hadjimatheou https://orcid.org/0000-0002-6848-7244

Notes

1. See the briefing offered to Essex Police and Crime Commissioners for a rare example a public-facing documents describing the Athena programme (Essex Police, Fire and Crime Commissioner, 2016).
2. Urban drug dealing networks that extend into regional markets.
3. Such practices tempt an extension, perhaps a stretching, of Cohen's piscary metaphor: policing ceases to be responsive and adopts a more speculative character. It becomes a 'fishing expedition'.

References

Alexander M (2012) *The New Jim Crow: Mass incarceration in an age of Colorblindness*. New York: The New Press.

Aradau C and Blanke T (2017) Politics of prediction: security and the time/space of governmentality in the age of big data. *European Journal of Social Theory* 20(3): 373–391.

Association of Chief Police Officers (ACPO) (2020) National digital policing strategy 2020–2030. Available at: https://www.apccs.police.uk/national-digital-policing-strategy-2020-2030/ (accessed 13 April 2025).

Bijker W, Hughes T and Pinch T (eds) (1987) *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. Cambridge, MA: MIT Press.

Brayne S (2021) *To Predict and Surveil*. Oxford: Oxford University Press.

Button M (2019) *Private Policing*. Routledge.

Byrne J and Marx G (2011) Technological innovations in crime prevention and policing. *Cahiers Politiestudies Jaargang* 2011–3(20): 17–40.

Cohen S (1985) *Visions of Social Control*. Cambridge: Polity.

CoPaCC (2018) Police ICT user perspectives. *Policing Insight*. Available at: https://policinginsight.com/reports/police-ict-user-perspectives-2018/ (accessed 22 January 2024).

Deleuze G and Guattari F (1987) *A Thousand Plateaus: Capitalism and Schizophrenia*. Minneapolis: University of Minnesota Press.

Egbert S and Leese M (2021) *Criminal Futures: Predictive Policing and Everyday Police Work*. London: Routledge.

Ericson R (1994) The division of expert knowledge in policing and security. *British Journal of Sociology* 45(2): 149–175.

Essex Police, Fire and Crime Commissioner (Essex PFCC) (2016) Athena Briefing Report for Police and Crime Commissioner Candidates. Available at https://www.essex.pfcc.police.uk/wp-content/uploads/2016/02/ATHENA-BRIEFING-FOR-PCC-CANDDIATES-100216.pdf.

Ewald F (2002) The return of Descartes's malicious demon: An outline of the philosophy of precaution. In: Baker T and Simon J (eds) *Embracing Risk, the Changing Culture of Insurance and Responsibility*. Chicago: The University of Chicago Press, 273–302.

Ferguson A (2017) *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York: NYU Press.

Flyverbom M (2024) Theorizing data analysis platforms – digital refractions and reconfigurations of pasts, presents and futures. *Information, Communication & Society* 27(13): 2366–2380.

Foucault M (2004) *Society Must Be Defended, Lectures at the Collège de France 1975–1976*. New York: Penguin.

Foucault M (2007) *Security, Territory, Population, Lectures at the Collège de France 1977–1978*. Basingstoke: Palgrave.

Fussey P, Davies B and Innes M (2021) 'Assisted' facial recognition and the reinvention of suspicion and discretion in digital policing. *The British Journal of Criminology* 61(2): 325–344.

Fussey P and Roth S (2020) Digitizing sociology: continuity and change in the internet era. *Sociology* 54(4): 659–674.

Hadjimatheou K (2021) Big tech and policing are shielded behind commercial confidentiality – it's a problem. *The Conversation*. Available at: https://theconversation.com/relationship-between-big-tech-and-policing-is-shielded-behind-commercial-confidentiality-its-a-problem-163958 (accessed 19 June 2024).

Hadjimatheou K and Nathan C (2022) Predictive Policing. In: Veliz C (ed) *Oxford Handbook of Digital Ethics*. Oxford: Oxford University Press, 433–448.

Heidegger MB, Time JM and Robinson E (1962) *(trans)*. Oxford: Basil Blackwell.

Hunter D, Mccallum J and Howes D (2019) Defining Exploratory-Descriptive Qualitative (EDQ) research and considering its application to healthcare. *Journal of Nursing and Health Care* 4(1).

Hutchby I (2001) Technologies, texts and affordances. *Sociology* 35(2): 441–456.

Kaufmann M, Egbert S and Leese M (2019) Predictive policing and the politics of patterns. *The British Journal of Criminology* 59(3): 674–692.

Lacey N (2013) The rule of law and the political economy of criminalisation: an agenda for research. *Punishment & Society* 15(4): 349–366.

Latour B (2005) *Reassembling the Social: An Introduction to Actor-Network-Theory*. New York: Oxford University Press.

Lemke T (2021) *The Government of Things: Foucault and the New Materialisms*. New York: NYU Press.

Lowman RJ, Menzies T and Palys S (eds) (1987) *Transcarceration: Essays in the Sociology of Social Control*. Gower Press.

Lyotard F (1984) *The Postmodern Condition: A Report on Knowledge*. Manchester: University of Manchester Press.

Marx G (2002) What's new about the "New surveillance"? Classifying for change and continuity. *Surveillance and Society* 1(1): 9–29.

NEC (2021) Press release. https://www.nec-enterprise.com/newsroom/press-releases/northgate-public-services-becomes-nec-software-solutions.

NEC (2022) Case Study: Athena Collaboration Programme. Available at: https://www.necsws.com/case-studies/public-safety/police/athena-collaboration-programme (accessed 16 January 2024).

NEC (n.d.) Police records management system. Available at: https://www.necsws.com/solutions/operational-police-software/police-records-management-system (accessed 16 January 2024).

Nellis M, Beyens K and Kaminski D (eds) (2013) *Electronically Monitored Punishment*. London: Wilan.

Newell B (ed) (2021) *Police on Camera: Surveillance, Privacy and Accountability*. Oxford: Routledge.

Pickering A (1995) *The Mangle of Practice: Time, Agency, and Science*. Chicago: University of Chicago Press.

Rutherford A (2000) An elephant on the doorstep: criminal policy without crime in New Labour's Britain. In: Green P and Rutherford A (eds) *Criminal Policy in Transition*. Oxford: Hart, 261–284.

Valverde M (2010) Questions of security: a framework for research. *Theoretical Criminology* 15(1): 3–22.

Wendt A (2015) *Quantum Mind and Social Science: Unifying Physical and Social Ontology*. Cambridge: Cambridge University Press.

Author biographies

Katerina Hadjimatheou, Senior Lecturer in Criminology, University of Essex.

Pete Fussey, Professor of Criminology, University of Southampton.