Missed Opportunities in Digital Investigation

First Author[1][Pat Thompson] and Second Author[2][Mark Manning] https://orcid.org/0000-0001-7772-2704

[1] University of Suffolk. Ipswich, UK. IP4 1 QJ

P.Thompson5@uos.ac.uk
Mark.Manning.1@uos.ac.uk

lncs@springer.com

Abstract.

A recent strategic review of policing published by the Police Foundation (Barber, 2020, p. 2) claimed that the police service in England and Wales is not equipped to meet the scale and complexity of the various challenges it faces, one of which involves the digital elements within crime investigation. Drawing upon data gathered for an MSc dissertation evaluating practices across investigators in the South of England, monthly samples from two years of serious crime investigations established that 50% of enquiries missed all digital investigative opportunities. Where a digital opportunity was identified, potential subsequent digital enquiries were missed 47% of the time. Whilst consistent with the Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMICFRS) (2018) and the Information Commissioners Office (ICO) (2020) reports which highlight that policing capability is lagging behind modern technology and affecting public confidence; these matters will be developed and discussed leading to the conclusion that, consistent with the police foundation report, loss of public confidence will undoubtedly damage police legitimacy.

Keywords: Digital, Investigative, Missed, Opportunities, Police, Legitimacy, Public, Confidence

1.0 Introduction

The context in which this paper will develop recognizes the rapid evolution and prevalence of complex digital elements within criminal investigations and how they may be stretching both the legitimate boundaries of the rule of law across state boundaries and also, policing by consent (Manning and Agnew, 2020). It will become clear that an investigative landscape fraught with technical and procedural complexities has evolved leading to deficiencies in the police use of digital investigation opportunities within police investigations. Previous research has identified the varying guises of these

complications which range from the ever-shifting developments in digital technologies affecting policing (National Police Chief's Council, 2016; Slessor, 2018. Shaw, 2018 and Dodd, 2019) to the complications experienced within a Criminal Justice System anchored within historical precedence (Enchev, 2011), and the increasingly informed expectations held by a technically educated public who simultaneously demand digital competence and digital privacy from law enforcement (Egawhary, 2019 and Trottier, 2015).

Whilst previous research has identified these layers of complexity, a research gap exists in establishing how these complexities manifest themselves within 'practice'. The study which informed this conference paper reviewed the use of four defined digital investigative techniques and examined whether investigators were identifying digital opportunities, applying them correctly and documenting their use so as to withstand judicial review and ultimately, public scrutiny within a criminal court. The findings indicated that a knowledge gap exists across investigators in identifying suitable lines of digital investigation. Where digital lines of enquiry were identified, questions have been raised as to the effectiveness of their application. The findings also established a lack of documented rationale being applied to the investigative decisions surrounding digital investigative opportunities.

2.0 The Field of Digital Policing

Changes to investigation procedures (McCartney & Shorter, 2019), digital evidence handling (Taylor et al, 2010), types of crime (Kirby & Penna, 2011) and the expectations placed upon investigators (Heaton, 2012) are just some examples of the increased investigative arena in which police investigations form part of a wider criminal justice service made up of multiple agencies and processes (Newburn, 2017). Complexity across these wider systems and processes compound upon a clear understanding of emerging technologies (Chan, 2001 and Levi & Leighton Williams, 2013). These complexities also straddle a landscape of differing policing priorities across the UK set by directly elected local Policing Crime Commissioners who drive policing policy (Raine and Keasey, 2012).

Brown (2015) comments upon the complexity of issues within digital forensics citing advances in technology, disparate legal jurisdictions and a list of agencies requiring knowledge of policing processes. However, digital forensics equates to only one aspect of investigations. Further examples include issues around the under-reporting of digital criminality (United Nations Office on Drugs and Crime, 2013) and the implications of technology on the legal profession and its functioning within courts (Wall and Johnson, 1997). These examples paint a picture of technology, investigating offences and processing investigative results through the criminal justice system as being fraught with complexity. This is highlighted by Owen (2018) who notes that technology outpaces policing knowledge whilst police knowledge simultaneously outpaces legislative

developments. McQuade (2006, p.41) also refers to policing tactics as co-evolving with technology and criminal ingenuity, and becoming increasingly complex, via '...recurring criminal and police innovation cycles which have a ratcheting-up effect akin to a civilian arms race'. The concept of a technological arms race is not unique to law enforcement. Hoffman (2015) identifies the complexities of emerging technology in medicine whilst Taddeo and Floridi (2018) explore the implications of artificial intelligence in warfare. Despite these "arms races" occurring across multiple sectors, perhaps unique to policing is the difficulty of matching tactics to offending and then presenting the results within a legal system rooted in historical precedent and tradition (Enchev, 2011) and to partner agencies who may not have technological parity with the police (Mishra et al.2011).

Further technical and cultural complexities are found within society at large and the expectations and objections that may be held by the public surrounding the use of digital tactics within investigations. A contemporary example of this is offered by Spinello (2019) who discusses the range of opinions surrounding the Federal Bureau of Investigations (FBI) attempts to "crack" the iPhones belonging to the 2015 San Bernadino terrorists (Braziel et al.2016) and the contrasting expectation of privacy for citizens versus the expectation to investigate terror offences. Set upon the backdrop of whistle blower Edward Snowden's revelations of widescale state sponsored surveillance style programs (Scheuerman, 2014), the public have developed a complex relationship with technology and information gathering whereby large swathes of the public willingly submit huge parts of their private lives to exposure on social media (Goodman, 2015), yet the trust held by the same public for "big tech" and government in using this data is low (Holmes and Burum, 2016). In the UK, organizations such as Liberty and Big Brother Watch also provide commentary against advances in law enforcement's use of technology (Big Brother Watch, 2017 and Liberty, 2019) whilst contrasting populist opinion suggests "If you have done nothing wrong, you have nothing to hide!" (Marwick and Hargittai, 2019).

These polarizing opinions are set within a context of increasingly available sources of information, which itself causes further complexity. Baum and Potter (2019) describe a disconnect between the vast availability of digital information and the levels of quality of the information available to the public. The voluminous availability of "fake news" has made the separation of fact from fiction in directing public opinion increasingly difficult (Hooper, 2019). When this phenomenon is applied to opinions surrounding policing and the criminal justice sector; news, fake news and opinion all add to an ever more complicated picture (Dentith, 2018 and Peters, 2018). The analysis of the expectations of digital tactic use within policing can be expanded further to explore the concept of "policing with consent" and whether this historical bedrock upon which the UK police have set their operational foundations is compatible with the pace and intrusive abilities of technology within investigations. Robertson (2016) describes policing as being consented to by the public or, at least acquiesced to, due to a lack of

understanding about what policing involves. The Home Office (2012) attempts to codify the concept of policing by consent by providing a list of generalized aspirational police behaviors and summarizing the concept as "the power of the police coming from the common consent of the public, as opposed to the power of the state". Curiously however the Home Office (2012) declare that it is not possible for a citizen to remove their consent.

These are all matters to be considered by the police service as they extend their reach into private matters through their use of technology. An example of this follows a recent trial of live facial recognition cameras by the London Metropolitan Police by Fussey & Murray (2019, p.125) who discuss incorrect facial identifications and the implications of this on public confidence into the police when they comment that its usage. The ethical implications of using technology in the deployment of police resources based on algorithmic decisions is one that has implications on the model of policing by consent. Whilst the accepted model of policing by consent has held sway, Shearing and Stenning (1983) previously posed long standing concerns about the emergence of private/public partnerships in law enforcement and how these mergers could affect the concept of consent.

Bayley (2016) considers the tradition of policing by consent by questioning whether the concept of consent requires a review of the levels of collaboration between the police and the public. Bayley (2016) posits however that this collaborative approach throws up its own complexities where the interests of the public, the police and public or private sector partners are all accounted for within a legal and operational model. These complexities are articulated by Sheptycki (2019, p.136) who considers that the "technopoly" mergers between police and private sector partners in tackling criminality through the use of technology is drifting into a pseudo-militaristic field and that this is increasingly '…the very opposite of democratic policing when an uncomprehending public experiences, a police presence that they do not endorse'. Whilst debate continues around the use of facial recognition technology by the UK police, Couchman (2019) highlights concerns regarding mass surveillance aided by questions as to who owns recorded facial "data", whilst Garvie and Frankle (2016) highlight issues of algorithmic racial discrimination.

It could be argued that public sector policing requires technical private sector collaborative support to provide the infrastructure and capability to keep pace with modern criminality, yet this opens a chasm between traditional notions of policing by consent and the concept of "technopoly" (an assumption that technology is always positive and of value; Segal, 1993). This shifting of the established notion of policing by consent invites polarized opinions from a more widely informed populace. In 2012, Bratton and Tumin described policing in Los Angeles as having been "run into the ground" with cuts to resources and equipment. Parallels to the recent period of austerity and the effects thereof on UK policing can be drawn (Manning and Agnew, 2020). In a contemporary publication, the Police Foundation (2020 p.54) highlights the current concerns

around public consent and policing stating that: in recent years, a tension has emerged between the shifting focus of policing and the views of the public. With police budgets and officer numbers cut, and the balance of risk shifting from public spaces and volume crime to online threats and hidden harm, many aspects of public facing 'core' policing have effectively been de-prioritized. As a result, concerns have begun to emerge about the health of the police "covenant" with the public.

The evidence would suggest that it is difficult, however, to reconcile an absolute operational necessity to deal with increasingly inventive criminality and persistently growing personal data sets with a public who demand, from a position of education and information availability, individual attention and accountability. Having accepted that law enforcement responses to evolving criminality and the handling of digital investigative products have become more complex, it is less clear how the digitization of criminality sits within the purview of police capability.

3.0 The Investigation of Digital Crime.

Some of the more well-known digital tactics used by investigators include, but are not limited to, the use of Automatic Number Plate Recognition (Home Office, 2019), the use of communications data (Home Office, 2015), the forensic analysis of digital devices (Van Baar et al. 2014) and the use of online research (Staniforth, 2016).

3.1 Open Source.

Online research, often referred to as open source investigation, is a valuable tool when investigating serious crime (Trottier, 2015 and Akhgar et al, 2017), though the use of open source tactics has resulted in complications in the development of policy and process at both local and national levels (Akhgar & Wells, 2018 and Nahn, 2008).

Complications include the necessity of policing agencies to adhere to legislation that was not written with the pace of the online developments in mind (Eskens et al. 2018). Complications are also created in considering how to balance the expectations of the public who are able to complete their own open source investigations, yet, who simultaneously demand privacy from law enforcement's use of open source methodologies (Egawhary, 2019 and Trottier, 2015). Indeed, publicly sourced investigations via social networks have been lauded by society at large yet deemed worrisome by the police following the use of open source tools linked to vigilante behavior (BBC, 2019). The ability of the public to investigate effectively via open source methodologies is both a blessing and a curse for law enforcement (Huey et al, 2013) who point to the lack of legal accountability in public investigations and a culture of skepticism within law enforcement as to the perceived benefits of public resources assisting in investigations.

The use of open source investigative methodologies has come under scrutiny by privacy campaigners. Ramakrishnan et al. (2014) reported on the use of social media aggregators in predicting civil unrest across Latin America. More recently the police use of social media to monitor protestors during the Extinction Rebellion protests has been called into question by Blowe (2019). The narrative against the monitoring and recording of data by authorities across social networks is echoed by the #FREESPEACHONLINE campaign hosted by Big Brother Watch (2019) who retain a stance of social media being the new "public forum" for discussion and therefore being protected from mass state snooping.

Whilst the police use of social media and open source research is limited to the prevention and detection of crime, perhaps cynicism around the leveraging of mass data sets by authorities has been fueled by recent exposés such as that around Cambridge Analytica (Cadwalladr and Graham-Harrison, 2018 and Isaak and Hanna, 2018). Recent commentary around data sharing between large technology companies and police agencies has also reinforced this nervousness with one recent article by Yoannou (2020) suggesting that Amazon was passing user details of "Ring" home camera systems to law enforcement along with remote access powers to allow the well intentioned switching on of cameras by police in the event of crime occurring in the locality of the device.

This cynicism about public / private partnership in harnessing and using social media in investigations can be balanced with a reported rise in complaints by victims to the police stating they have been abused in a social media space (Evans, 2015) and the accepted parallel of abuse and offending increasing across social media when high profile events such as terror attacks occur and are reported in the news (Müller and Schwarz, 2019). Seemingly law enforcement is expected by victims and the public to access social media during investigations and yet, the same victims and public are simultaneously cynical and suspicious of law enforcement engagement with social media companies and private sector partner organizations.

3.2 Digital Forensics.

The retrieval of evidence from digital devices, known as digital forensics, is defined by Pollitt (2004) as a process to identify, preserve, analyze, and present data from digital devices. As digital devices evolve, the extraction of evidential data has become more complex as noted by Leong (2006) and Agarwal et al. (2011) who highlight issues between the changing technological developments in digital devices and the separation of understanding between those who have become increasingly technical in the abstraction of information and those who have the responsibility of applying legal frameworks to any recovered evidence.

This is highlighted by Mackie et al (2017) who reference the skills of digital forensics teams versus the arrival of the European Union's General Data Protection Regulations (GDPR) and the complications of bringing the two perspectives into alignment.

Whilst this paper by Mackie et al (2017) was largely based on the premise of data breach offences within a corporate environment, a parallel can be drawn to advances in cloud technology, the emergence of new legislation (Investigatory Powers Act, 2016), and the complications of legally and technically retrieving cloud data, analyzing it correctly and presenting it in evidence. Developments in cloud technology has resulted in the holding of data on servers potentially anywhere in the world. Son et al. (2013) reference cloud providers placing cloud servers across the globe to allow for balancing of resources against global demand. Pătrașcu & Patriciu (2013) comment on the difficulties in retrieving data held in disparate locations and Ferguson et al. (2018) discuss that this global infrastructure alone provides "severe implications for the detection, investigation and prosecution" of offences.

These "severe implications" are compounded further by considerations surrounding the proportionality of seizure and analysis of devices (Beebe and Clark, 2005; Trenwith and Venter, 2013; Information Commissioner's Office, 2020) (hereafter ICO), the intrusion into data held on devices about persons not believed to be linked to criminality (Big Brother Watch, 2017) and the sheer volumes of data that needs to be stored by the police in the management of digital exhibits (Quick and Choo, 2014).

Certainly, issues surrounding the volumes of data recovered by police and the proportionate and relevant analysis of this data in crime investigations has led to adverse publicity, including data implications involving the collapse of the Liam Allan rape trial (Smith, 2018). The subsequent review of disclosure processes and the impact digital evidence has had on investigations and the court process identified unwieldy volumes of material and a lack of management of this data as having a negative impact across the criminal justice system (Attorney General's Office, 2018). The proposed solutions have led to more confusion across constabularies as police officers and investigators struggle to ensure understanding across seizure, analysis and presentation of digital evidence. This confusion is equally present within the Crown Prosecution Service and the courts (Bowcott, 2019). Criminal prosecutions within the UK rely on a burden of proof measured as "beyond reasonable doubt" (Newburn, 2017). Accordingly, the presentation and subsequent contesting of digital evidence in a court can be complicated without that evidence being corroborated by other means.

3.3 Communications Data.

One method of achieving corroboration of some elements of digital evidence is via communications data. Communications data is "the who, where, when and how of a communication" (Home Office, 2015). Whilst accessing and using communications data is a valid investigative tool, its use also affords an investigator the ability to corroborate other aspects of digital evidence. Communications data is largely comprised of records of traffic across the cellular network via mobile or land-line telephony. It can also comprise mobile internet traffic records as well as more esoteric versions of

communications including mobile app communications to companies such as “Uber” or “Just Eat”. The Investigatory Powers Act (2016) is the statutory framework that defines the circumstances and process by which investigators may apply for communications data. This process involves submitting a request which complies with the requirements of the act. This request is then triaged by a team who pass the request to an independent statutory body, “The Office for Communications Data Authorizations” (OCDA). OCDA’s responsibility is to grant or deny the request having considered whether the request is lawful, necessary and proportionate (Gov.uk, 2016. Forensic Analytics, 2019). The proportionate lawfulness of any request for communications data is subjective and requires individual interpretation of the law against the requirements of the request. Whilst OCDA will refer to this as balancing the proportionality of the request, Gill (2013) suggests this process involves the consideration of “sousveillance”, the considering of public perception as to where the power balance wielded by the state is held into the intrusion of the privacy of citizens.

As the Investigatory Powers Act (2016) progressed through its parliamentary approval process, Chivers (2015) stated that there was a need for “a discussion about what kind of surveillance is truly necessary and proportionate in an increasingly digitalized society”. Whilst legislators advised that the creation of the independent body OCDA would ensure that proportionality would remain in the forefront of communications data acquisition, others believed that the Investigatory Powers Act was a “snoopers charter” (Carlo, 2016).

In addition to the discussions surrounding privacy and proportionality, technical complexity exists in accessing and using communications data. Lock et al. (2013) reference the problems associated with the recording of communications data when routed through virtual private networks whilst Brown (2015) speaks to “advancements in the functionality of information communication technologies and disparities between systems of law globally” as challenging.

Further challenges then exist in the processing of gathered communications data. Issues with the computer systems used throughout the criminal justice service (Waterhouse, 2019 and Crown Prosecution Service, 2018) have rendered the effective transfer of data between agencies difficult due to the incompatibility of systems used. Despite these difficulties, communications data remains a critical line of enquiry in many investigations where the linking of communication events and identification of where these events occurred is crucial to successful investigations (May, 2015).

3.4 Automatic Number Plate Recognition (ANPR).

ANPR is described by Gunawan et al. (2017, p.1973) as ‘...an intelligent system which has the capability to recognize the characters on vehicle number plate’.

This recognition is then overlaid onto a location, mapping where the recognition took place. Rogers and Scally (2018) identify both the proactive and reactive abilities

of ANPR for the investigator. Rogers and Scally (2018) also identify the scale of ANPR use across the UK police establishment commenting that cameras exist on nearly all major road networks. Wright (2016) corroborates that as far back as 2012, over eleven billion records of vehicle movements had been captured by the ANPR camera network.

This volume of data brings a layer of complexity to investigations surrounding the storing of images and associated vehicle, keeper and location data for an exponentially increasing data set (Jaques, 2015. Akhgar and Yates (2013, p.155) develop this further stating that in dealing with "big data sets" there is a requirement for '…a specific combination of tools, intel., experts and data sources along with the suitable access protocols and security solutions.'

The pattern of law enforcement difficulty with advances in technology is prevalent across all digital tactics discussed thus far. The other consistent parallel across tactics has been law enforcement's grappling with the concepts of privacy and proportionality and the varied expectations held by an increasingly vocal and digitally aware public. This theme is present across ANPR data capture and manipulation also.

Big Brother Watch (2013) comment on the exponentially increasing scale of police use of ANPR data and the possible consequences of not maintaining track of police marking of the data whilst Woods (2017) debates the notion that the use of ANPR data acts as an intrusion into the private lives of road users when set against both the European Convention on Human Rights and the European Union Charter.

It is acknowledged that policing has an ever-expanding remit (Millie, 2013 and Millie & Bullock, 2012). It is argued that this expansion, alongside Governmental ambitions to move policing from an "unskilled" vocation to being a formal profession (Brown et al, 2018), has led to a debate as to the overall identity and mission of the police. Amidst this identity crisis, developing measurable and successful process in the already complicated digital arena is difficult. Speaking to private sector management processes and measuring performance, Magretta and Stone (2002) questioned; "given our mission, how is our performance going to be defined?". It is unclear how policing can answer this question.

4.0 Method.

Using a County Constabulary within England as a case study, research was conducted which aimed to understand both the practical use of digital investigative tactics within 'serious crime investigations' and whether the proportionate use of such tactics was considered when they were applied.

The term serious crime was used in the sense that it is defined in statute by the Police Act 1997. (National Archives, 2006 and Police Act,1997)

The research afforded an opportunity to explore the identified knowledge gap including topics of particular interest including: Identifying the levels of use of digital investigative tactics and establishing where opportunities are commonly missed; where

digital tactics are used, establishing the levels of understanding held by investigators into the practical application of digital investigative techniques; establishing the levels of understanding of the proportionate use of digital investigative techniques; within the case study, to what extent are identified digital investigation techniques being used and understood within serious crime investigations?

This research analyzed secondary data from completed investigations as opposed to 'live' investigations. Completed investigations can be interrogated for information whereas the dynamic nature of "live" investigations risks missing the measurement of digital tactic use which may become a valid tactic later in an enquiry and therefore missed by snapshot analysis.

All of the data already existed within the policing systems of the area under research, having been collected as part of a different original purpose. One benefit of using existing data in identifying the use of digital tactics was that the investigative process was not biased by the investigator's awareness of researcher scrutiny. This knowledge may have led to the investigator including tactics that they would previously not have considered and the resulting data not being representative of the 'norm' for participants.

4.1 Data collection procedures.

The 2019 Crime Survey of England and Wales identified 60,920 crimes in the year ending March 2019 for this particular Constabulary, not including fraud offences (Office for National Statistics, 2019).

Utilizing the Constabulary's crime recording system, a structured query could be leveraged identifying only those reported offences which resulted in an investigation taking place.

It is acknowledged that not all reported crimes result in investigations (Hymas, 2019). Comparing the extracted investigations against the Home Office list of serious crimes identified which of the extracted investigations fell within the serious crime definition. Having identified a data set of crime investigations, it was necessary to identify a time period from which to collect a sample from the data.

On the understanding that 60,920 crimes were reported in year ending March 2019, it was necessary to establish how many of these resulted in investigations and subsequently, how many resulted in serious crime investigations which would produce a sample set from which to select data for this research.

The following data collection process was established:

1) All crime investigations between January 2018 and December 2019 inclusive were extracted totaling a sample size of 13,377 investigations. were exported from this two-year period. The data was cleansed and just the crime reference numbers, and offence types recorded.

2) The Home Office list was filtered so that all offences that did not satisfy the statutory condition of potentially carrying a custodial sentence of three years or under were removed.

3) Several offences that matched the definition of serious crime remained yet would traditionally never fall within the practicalities of serious crime investigation were removed. The rationale behind these removals were that, for example, by definition, a theft offence can carry a seven-year custodial sentence, thereby defining it as "serious". A shoplifting offence however would not be considered a "serious crime" from an investigative perspective and therefore would be outside the scope of this research. This rationale is supported by the Cambridge Harm Index (Sherman et al. 2016) which suggests that not all crimes are "created equal" and that measures of seriousness can be applied to crime recording. For this research, offences have been removed which would all but exclusively be dealt with at Magistrate's court and therefore never attract the serious crime sentencing powers (Sentencing Council, 2020).

4) Having filtered out offences not attracting a custodial sentence of over three years and offences not traditionally within the remit of serious crime investigations, a total of 2,275 investigations remained as in the sample providing a mean number of serious crime offences per month across the twenty-four-month sample period of 94.79.

A random selection of four investigations per month over the sample period yielded 96 investigations selected, the equivalent to an average month's serious crime investigations.

4.2 Data Analysis.

Having identified 96 investigations, an analysis process was developed to capture the relevant quantitative and qualitative data required better understand the approach taken to digital elements within investigations. This analysis process is visualized in **Figure 1 below**:

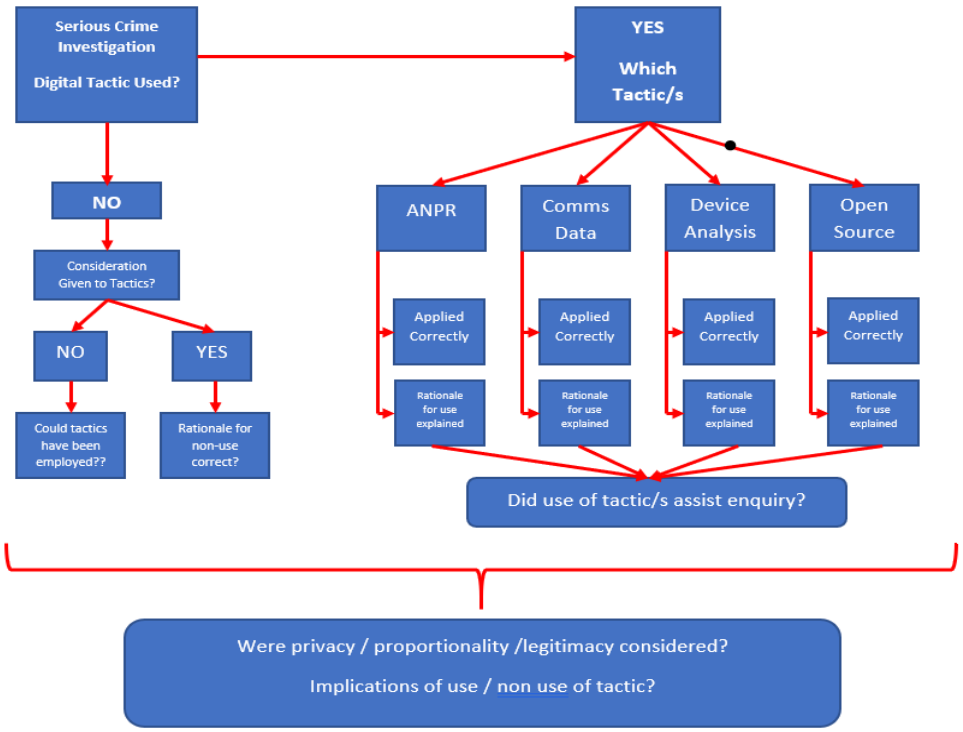

Figure 1 – Data analysis flowchart.

4.3 Results.

Quantitative analysis of the results identifies that

- From the 96 serious crime investigations: 29 investigations did not contain circumstances where digital lines of enquiry were available or viable.
- Of the remaining investigations, 19 correctly identified one or more digital lines of enquiry. 48 investigations missed all possible digital lines of enquiry.
- 53 investigations (55%) were dealt with by officers in non-detective roles, whilst 43 investigations (45%) were dealt with by officers in detective roles.
- Within the 19 investigations where digital tactics were identified, there were instances of multiple tactics being used, with a total of 28 recorded usages of one or more of the digital tactics noted across these 19 investigations.
- Out of the 19 investigations that did apply digital tactics, it was noted that 9 of them (47.3%) missed further digital investigative opportunities having identified an initial opportunity. Of the 48 investigations which missed all digital

investigative opportunities, 16 (33.4%) were missed by officers in detective roles whilst 32 (66.6%) were missed by officers in non-detective roles.

- Of the 28 recorded usages of digital tactics, 27 of them appear to have been technically applied correctly. Of the 28 recorded usages of digital tactics, 16 (57%) of them described a rationale for the use.
- Within the 48 investigations where digital enquiries were not used, the rationale for the lack of use was recorded once for each of the identified tactics.
- The legitimacy / proportionality aspects of digital tactic use were explained on 1 occasion each for the use of communications data, device analysis and open source tactics.

Qualitative analysis of the results provides the following insight into the use of (or not) of digital investigative tactics.

- Evidence existed of officers correctly identifying digital lines of enquiry, one example being an investigating officer correctly identifying that a mobile device required a more forensic download than was locally available and another officer identifying that ANPR searches could offer investigative lines of enquiry in overlaying data with a missing persons records system whereby receipts and a car parking ticket were recovered from a vehicle.

- Evidence existed of investigators incorrectly identifying digital lines of enquiry including wrong rationale for the non-utilization of ANPR searches as being given as there being insufficient cameras in an area and a time frame being too wide to provide meaningful search parameters.

- Evidence was present of the use of rationale in the consideration of use (or non-use) of digital investigative tactics including an example whereby an investigator identified issues with the accuracy of information held by the police and that this would therefore prevent the initial use of communications data applications.

- A further example demonstrates a rationale for the seizure of a victim's phone handset, the policing powers used and level of intrusiveness in searches based on quantity of data extracted. The rationale also details an explanation for the seizure and examination of the suspect's device and goes onto identify complications and missing data from these initial reviews which developed a rationale for further digital investigative work on the handsets.

- Evidence identified examples of digital investigative opportunities existing in enquiries which were missed by investigators despite the victim providing the

investigator with signposting as to how to conduct relevant digital enquiries. Evidence also existed of digital enquiries not being progressed due to problems around a lack of time or an increased workload.

- These capacity issues were highlighted repeatedly and within a local area, a prioritisation process around which crimes will be dealt with and in which order was instigated, often to the detriment of progressing entirely viable digital lines of enquiry. This was adopted both by investigators and their supervisors.

- Evidence also existed of investigators not maximising the use of digital investigative methods to understand the "wider picture" including an example involving a domestic abuse offence where the investigator did not identify that more than one offence had been committed and a separate stalking report where only a single incident was investigated as opposed to the wider reported behaviours.

- Despite these problems, there also existed evidence of investigative tenacity despite digital complications including an example whereby an investigator has continued to pursue digital lines of enquiry despite initial attempts to glean evidence being frustrated by the technical architecture of the application being reviewed.

5.0 Discussion.

The results presented from this evaluative research established a number of areas of discussion.

5.1 Missed Opportunities.

The prevalence of missed digital investigative opportunities clearly identifies an area of weakness across investigations. It is, however, difficult to identify where this weakness specifically stems from.

Some of the sampled offences identified a lack of time or an increased workload as a reason as to why digital opportunities were missed.

This is consistent with recent HMICFRS reporting (Her Majesty's Chief Inspector of Constabulary, 2018) which highlighted that a lack of capacity across investigators and police officers identified "a widening gap between the needs of the public and the police's capacity and capability to meet them".

Whilst it is accepted that lack of capacity is a partial element in the non-identification of digital lines of enquiry, it is suggested that capacity takes a less prominent role to a lack of understanding of the opportunities available in the investigation of digital elements of crime.

The same HMICFRS report (2018, p.33), backed up by the recent ICO (2020) report identifies deficiencies in the digital elements of investigations: As long as the police persist in using 20th-century methods to try to cope with 21st-century technology and ways of life, they will continue to fall further and further behind, and the quality of justice will exponentially diminish.

This cultural difficulty in keeping pace with technology can be conceptually linked to the "Dunning-Kruger Effect" (Dunning 2011); the notion that if an investigator doesn't know what opportunities are available to them in investigating crime, they would be unlikely to identify the opportunities in their investigations. This lack of knowledge, when embedded within a culture that is "using 20th-century methods to try to cope with 21st-century technology", can perhaps explain why there is such a high number of missed opportunities.

In one of the above noted examples, an exasperated victim who has been told that no further enquiries will be completed into the matter despite that victim identifying digital lines of enquiry to the investigating officer. Williams (2017) discusses the public's expectation of police to tackle open source enquiries. In the example, the victim identifies communications data opportunities alongside Facebook enquiries, opportunities which have alluded the investigator. This level of education and expectation amongst the public, when faced with non-action by the police in investigating reports of crime, decreases public trust and confidence in the police.

Morell et al. (2020) suggest that one element of maintaining trust between the public and the police is to ensure that the public believe that the police are competent. In this instance, the belief of the victim is that the police are not competent. Jackson et al. (2011) suggest that "when people are aligned with their society's legal structures, they are … more likely to assist the police and courts through reporting crimes, identifying culprits, and giving evidence".

The above circumstances identify how missed opportunities amongst an educated public can erode trust in the police. These missed opportunities are believed to be down to a lack of knowledge (Honess, 2020) and the cultural lack of modernity around policing practices (Her Majesty's Chief Inspector of Constabulary, 2018).

Allocation Policies.

Despite the filtering process applied to ensuring that only serious crime made up the research sample, a larger proportion of the sample were investigated by non-detective resources. These investigations included offences such as supplying of class A drugs, sexual assaults, fraud, and stalking offences.

The Cambridge Harm Index (Sherman et al. 2016) acknowledges that not all crimes are created equally and proposes a "weighting" assessment to understand the potential harm which could be experienced from the commission of an offence.

Whilst the sample indicates that the greater number of investigations were allocated to non-detective resources, those that could be said to be of a higher harm weighting (for example rape and offences against vulnerable persons) attracted detective resources.

This can be viewed as a positive given that the sample data indicates that non-detective resources miss more digital investigative opportunities than detective resources. What the allocation process does not seem to identify however, are the potential harmful offences that start at a lower harm threshold yet repeat into a higher harm set of circumstances. The tragic case of Fiona Pilkington in 2007 highlighted that the culmination of multiple lower harm crimes can have devastating effects.

In examples given above, investigators have missed digital enquiries which would have revealed patterns of stalking behaviors or repeated domestic abuse offences, and whilst these are "serious crime" offences that would not necessarily attract detective resources, the implications of missing digital evidence which evidences ongoing domestic abuse and controlling behaviors have been repeatedly highlighted (Office for National Statistics, 2019; Grierson, 2020). It is suggested that had efforts been put into the recovery of digital evidence across these examples, the investigator would have been in a better position to risk assess and address relevant future safeguarding actions.

This lack of awareness or ability to identify digital lines of enquiry amongst non-detective resources has the potential to not only miss investigative and safeguarding opportunities, but to also erode at the public's confidence in the police's ability to investigate effectively. Whilst it is difficult to argue against prioritizing high-risk crimes against lower risk fraud offences, it is suggested that by not engaging fully in the pursuit of these crimes, officers do not learn how to develop skills in the digital investigative arena, thus reinforcing the previously referenced "Dunning-Kruger Effect" and simultaneously continuing to erode the confidence of the public into the police's abilities and legitimacy.

5.2 Digital enquiries Applied Correctly.

What is clear from the sample data is that some officers do take a positive approach to digital enquiries and will not be put off by inevitable digital complications that may arise.

The example noted above whereby an investigator continued to pursue digital lines of enquiry despite initial attempts to glean evidence being frustrated by the technical architecture of the application being reviewed demonstrates that with a willingness to pursue and learn, digital enquiries can be productive.

6.0 Rationale and Legitimacy.

Following the collapse of the Liam Allan rape trial in 2017, scrutiny into how investigators apply rationale to their enquiries, especially around elements of digital investigation, has been the subject of much discussion. Smith (2018, p.12) suggests in relation to the Liam Allen trial that: Whatever the rationale for the approach of the OIC, the material should have been scheduled and by failing to do so the CPS were denied an accurate picture of the case, leading to a flawed charging decision.

The evidence from this research suggests that it is a minority of investigators who are applying a digital rationale within investigations. Given the increasing relevance of digital data in investigations, it is suggested that documenting a rationale detailing the reasons for completing or not completing digital enquiries is as important as the investigation itself, and to miss this could lead increasingly to adverse conclusions not only within the criminal justice system but also affecting the public's wider view of the police.

The lessons from the Liam Allan case, proposed by the Attorney General's Office (2018) do not seem to have filtered through to operational investigators. Whilst organizations such as Liberty and Big Brother Watch continue to publicly scrutinize law enforcement's use of technology, it is increasingly important for investigators to document a rationale, reasoning what digital enquiries are available and why they are or are not being pursued. The implications of not doing so may see repeated collapses of prosecutions and increasingly negative public scrutiny, all of which cyclically feeds back into questions around the ability of police to continue to operate with the full consent and support of the public whilst accessing the public's digital data.

This question around policing across digital data and the intrusiveness of the investigative tactics can be framed against Bayley's (2016, p.167) argument that: 'policing with consent' must be rethought because the public increasingly wants direct rather than representative participation in the supervision of the police. Documenting a rationale around digital investigations requires liaison with the public to ensure that the public's consent and support is maintained. A rape victim, for example, may consent to having phone messages accessed and reviewed by investigators, but not pictures. Notwithstanding the technical complexities around this (for example, is Instagram a messaging application, an image application or a hybrid of both?), it is necessary for an investigator to balance the wishes of the victim against the evidential elements of the enquiry and the potential of scrutiny and cross examination as to investigative decisions at a later judicial hearing. This is a theme noted by the information Commissioner's Office (2020) where 13 recommendations were made to constabularies around the balancing of data protections expected by the public and the competing statutory frameworks found within the criminal justice system.

Bradford (2014) suggests that “the actions of police officers can have a profound effect on the legitimacy of the police”. In the context of digital investigations, it could be argued that this cycle evidences a social positive feedback loop whereby publicly failing prosecutions increase public uncertainty over law enforcement’s capability and competence with digital evidence. This in turn increases public scrutiny which in turn uncovers more failings. All these factors serve to augment each other.

6.0 Conclusions.

This research has illustrated the complexity that surrounds police use of digital investigative tactics.

Complexities exist within the technical arena however perhaps more pressing are the complexities around applying the evolving pace of the modern digital world to a historically rooted criminal justice system that bases its judgements and future decisions on that of precedent. Adding to this is the public’s increased knowledge of modern-day digital capabilities and the resultant expectations of law enforcement in being able to access data and process it effectively yet to simultaneously maintain privacy and to remain defensible against accusations of “big brother” interventions. These layers of complexity then feed into questions as to how UK policing can ensure that it retains legitimacy with the public and, ultimately, as to whether or not the digital elements of investigative work accord with the long-standing tradition of “policing by consent”.

This research has identified that whilst a small number of investigators have an interest and an ability to positively identify and pursue the digital elements of serious crime investigations, a majority of investigators do not. This lack of ability speaks loudly to the questions posed around the legitimacy of the police and the ability of law enforcement to command the confidence of the public and ultimately to police with their consent.

This research has also identified that whilst serious crimes carrying the highest risk are largely allocated to detective resources, what could be termed as “volume -serious crime” is often allocated to non-detective resources, where the largest amount of digital opportunities are missed. As has been highlighted, it is within these cases that tragedies such as that of Fiona Pilkington are found.

This research has highlighted that despite some officers making relevant digital enquiries, the documenting of the rationale behind these enquiries is largely lacking. It is difficult to quantify the lack of a rationale behind a missed digital opportunity – has it been missed through a lack of knowledge or through choice? In either event, the lack of an accompanying rationale can have serious consequences and it exposes issues surrounding the police and their perceived legitimacy when dealing with digital enquiries.

References

Agarwal, A., Gupta, M., Gupta, S. and Gupta, S.C.: Systematic digital forensic investigation model. International Journal of Computer Science and Security 5(1), 118-131 (2011)

Akhgar, B., Bayerl, P.S., Sampson, F: Open Source Intelligence Investigation: From Strategy to Implementation. Springer, (2017)

Akhgar, B., Wells, D.: Critical success factors for OSINT Driven Situational Awareness. European Law Enforcement Research Bulletin, 18 (2018)

Akhgar, B., Yates, S.: Strategic Intelligence Management, National Security Imperatives and Information and Communications Technologies. Butterworth, Heinemann, US (2013)

Attorney General's Office, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/756436/Attorney_General_s_Disclosure_Review.pdf, last accessed 2020/3/4.

Barber, Sir, M.: The First Report of The Strategic Review on Policing in England and Wales. Police Foundation, (2020).

Baum, M.A., Potter, P.B.: Media, public opinion, and foreign policy in the age of social media. The Journal of Politics, 81(2), 747-756 (2019).

Bayley, D.H.: The complexities of 21st century policing. Policing: A Journal of Policy and Practice, 10(3), 163-170 (2016).

BBC, https://www.bbc.co.uk/news/uk-england-50302912, last accessed 2019/11/28.

Beebe, N., Clark, J.: Dealing with terabyte data sets in digital investigations. In: IFIP International Conference on Digital Forensics, pp. 3-16. Springer, Boston, MA. (2005).

Big Brother Watch, https://bigbrotherwatch.org.uk/wp-content/uploads/2013/03/ANPR-Report.pdf, last accessed 2020/03/08.

Big Brother Watch, https://bigbrotherwatch.org.uk/wp-content/uploads/2017/11/Police-Access-to-Digital-Evidence-1.pdf, last accessed 2020/02/17.

Big Brother Watch, https://bigbrotherwatch.org.uk/campaigns/freespeechonline/#introduction, last accessed 2020/02/28.

Blowe K, https://freedomnews.org.uk/police-surveillance-a-note-for-extinction-rebellion-campaigners, last accessed 2020/02/28.

Bowcott, O, https://www.theguardian.com/law/2019/may/01/explosion-in-digital-evidence-has-left-cps-struggling-says-union, last accessed 2020/03/04.

Bradford, B.: Policing and social identity: Procedural justice, inclusion and cooperation between police and public. Policing and society 24(1), 22-43 (2014)

Bratton, W. & Tumin, Z.: Collaborate or Perish!: Reaching Across Boundaries in a Networked World. Crown Business, 16-79 (2012).

Braziel, R., Straub, F., Watson, G., Hoops, R.: Bringing calm to chaos: A critical incident review of the San Bernardino public safety response to the December 2, 2015, terrorist shooting incident at the Inland Regional Center. In: United States. Department of Justice, Office of Community Oriented Policing Services. United States. Department of Justice. Office of Community Oriented Policing Services (2016).

Brown, C.S.D.: Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. International Journal of Cyber Criminology 9(1), 55-119 (2015).

Brown.: Extending the remit of evidence-based policing. International Journal of Police Science and Management 20 (1), 38-51 (2018).

Cadwallader., Graham-Harrison, E.: Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian, 17, 22 (2018).

Carlo, S, https://www.independent.co.uk/voices/snoopers-charter-theresa-may-online-privacy-investigatory-powers-act-a7426461.html, last accessed 2020/03/06.

Chan, J.B.L.: The Technological Game: How Information Technology is Transforming Police Practice. Criminology & Criminal Justice 1(2) 139-159 (2001).

Couchman, H, https://www.libertyhumanrights.org.uk/sites/default/files/Liberty%27s%20Briefing%20on%20Facial%20Recognition%20-%20October%202019.pdf, last accessed 2020/02/21.

Crown Prosecution Service, https://www.cps.gov.uk/legal-guidance/disclosure-guidelines-communications-evidence, last accessed 2020/12/08.

Dodd, V, https://www.theguardian.com/uk-news/2020/feb/26/extra-officers-must-lead-to-less-priti-patel-tells-police-chiefs, last accessed 2020/03/10.

Dunning, D.: The Dunning–Kruger effect: On being ignorant of one's own ignorance. In: Advances in experimental social psychology 44, 247-296 (2011)

Egawhary, E.M.: The Surveillance Dimensions of the Use of Social Media by UK Police Forces. Surveillance & Society 17(1), 89-104. (2019).

Eskens, S., Van Daalen, O., Van Eijk, N.: 10 Standards for Oversight and Transparency of National Intelligence Services. Journal of National Security Law & Policy 8(3), 1-38 (2016).

Entchev, I.: A Response-Dependent Theory of Precedent. Law and Philosophy 30(3), 273-290 (2011).

Evans, M.: Police facing rising tide of social media crimes. Telegraph. 20156/15

Ferguson, I., Renaud, K. and Irons, A.: Dark Clouds on the Horizon: The Challenge of Cloud Forensics. Cloud Computing, 61 (2018).

Forensic Analytics: https://www.forensicanalytics.co.uk/the-investigatory-powers-act-and-access-to-comms-data/, last accessed2019/12/17.

Fussey, P. and Murray, D.: Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology. Human Rights Centre, University of Essex (2019).

Garvie, C. & Frankle, J.: Facial-recognition software might have a racial bias problem. The Atlantic, 7 (2016).

Gill, P.: Should The Intelligence Agencies 'Show More Leg' or Have They Just Been Stripped Naked? Information & Security 30(1), 11-31 (2013).

Goodman, M.: Future crimes: Inside the digital underground and the battle for our connected world. Random House, (2015).

Gov.uk, https://www.gov.uk/government/organisations/office-for-communications-data-authorisations/about, last accessed 2019/12/17.

Grierson, J.: https://www.theguardian.com/society/2020/apr/15/domestic-abuse-killings-more-than-double-amid-covid-19-lockdow, last accessed 2020/06/04.

Gunawan, T.S., Mutholib, A., Kartiwi, M.: Performance Evaluation of Automatic Number Plate Recognition on Android Smartphone Platform. International Journal of Electrical and Computer Engineering vol 7(4),1973.

Heaton, R.: Police Resources, Demand and the Flanagan Report. The Police Journal, 1-22 (2012).

Her Majesty's Chief Inspector of Constabulary, https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/state-of-policing-2018.pdf, last accessed 2020/06/03.

Hofmann, B.M.:Too much technology. British Medical Journal 16 (2) , 705 (2015).

Holmes, P.G. & Burum, S.: Apple v. FBI: Privacy vs. Security? In. National Social Science Proceedings 62 (1), 24-41 (2016).

Home Office, https://www.gov.uk/government/publications/policing-by-consent/definition-of-policing-by-consent, last accessed 2020/02/18.

Home Office, https://www.gov.uk/government/collections/communications-data, last accessed 2019/11/10.

Home Office, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/806674/NASPLE_-_January_2019_ last accessed 2019/11/10.

Honess, R.: Mandatory Police Training: The Epitome of Dissatisfaction and Demotivation? Policing: A Journal of Policy and Practice, (2020).

Hooper, V.: Addressing the Challenge of Guiding Our Students on how to Deal with Fake News. In. InSITE 2019: Informing Science+ IT Education Conferences: Jerusalem, 021-032 (2019)

Huey, L., Nhan, J. and Broll, R.: Uppity civilians' and 'cyber-vigilantes': The role of the general public in policing cyber-crime. Criminology & Criminal Justice, 13(1), 81–97 (2013).

Hymas, C, https://www.telegraph.co.uk/politics/2019/04/23/police-chief-admits-60-per-cent-crime-not-fully-investigated/, last accessed 2020/04/21.

Information Commissioner's Office, https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf, last accessed 2020/07/29.

Investigatory Powers Act (2016)

Isaak, J. & Hanna, M.J.: User data privacy: Facebook, Cambridge Analytica, and privacy protection. Computer 51(8), 56-59 (2018).

Jackson, J., Bradford, B., Hough, M., Kuha, J., Stares, S., Widdop, S., Fitzgerald, R., Yordanova, M., Galev, T.: Developing European indicators of trust in justice. European Journal of Criminology 8 (4), 267-285 (2011).

Jaques, P, https://www.policeprofessional.com/news/huge-volume-of-visual-evidence-puts-investigators-under-extra-pressure/, last accessed 2019/12/20.

Kirby, S. & Penna, S.: Policing mobile criminality: implications for police forces in the UK, Policing. An International Journal of Police Strategies & Management 34 (2), 182-197 (2011).

Leong, R.S.: FORZA–Digital forensics investigation framework that incorporate legal issues. Digital Investigation 3, 29-36 (2006).

Levi, M. & Leighton Williams, M.: Multi-agency partnerships in cybercrime reduction: Mapping the UK information assurance network cooperation space. Information Management & Computer Security 21(5), 420-443 (2013).

Liberty Human Rights, https://www.libertyhumanrights.org.uk/news/press-releases-and-statements/liberty-client-takes-police-ground-breaking-facial-recognition, last accessed 2020/02/17.

Lock, R., Cooke, L. & Jackson, T.: Online Social Networking, Order and Disorder. Electronic Journal of E-Government, 11(2), 229-240 (2013).

Mackie, J., Taramonli,. Bird, R.: Digital Forensics and the GDPR: Examining Corporate Readiness". In: European Conference on Cyber Warfare and Security, , pp. 683-691. (2017).

Magretta, J. & Stone, N.: What Management is: How it Works and Why it's Everyone's Business. Free Press, New York, NY (2002).

Manning, M. & Agnew, S.: Policing in the era of AI and Smart Societies: Austerity; Legitimacy and Blurring the Line of Consent. In: Jahankhani, H.; Akhgar, B.; Cochrane, P., Dastbaz. M.: Policing in the Era of AI and Smart Societies. Springer (2020).

Marwick, A & Hargittai, E.: Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online. Information, Communication & Society 22(12), 1697-1713 (2019).

Home Office: Statement to Parliament: Home Secretary: Publication of draft Investigatory Powers Bill. November 4, 2015. House of Commons, London (2015).

McCartney, C. & Shorter, L.: Police Retention and Storage of Evidence in England and Wales. International Journal of Police Science & Management (2019).

McQuade, S.: Technology-enabled Crime, Policing and Security. The Journal of Technology Studies 32 (1), 32-42 (2006).

Millie, A.: The policing task and the expansion (and contraction) of British policing. Criminology & criminal justice 13(2), 143-160 (2013).

Millie, A. & Bullock, K.: Re-imagining policing post-austerity. British Academy Review 19, 16-18 (2012).

Mishra, J.L., Allen, D.K., Pearman, A.D.: Information sharing during multi-agency major incidents. Proceedings of the American Society for Information Science and Technology 48(1), 1-10 (2011).

Morrell, K., Bradford, B. & Javid, B.: What does it mean when we ask the public if they are 'confident' in policing? The trust, fairness, presence model of 'public confidence. International Journal of Police Science & Management 22 (2), 111-122 (2020).

Müller, K. & Schwarz, C.: Fanning the flames of hate: Social media and hate crime. SSRN Electronic Journal 3082972 (2019).

National Archives, http://www.legislation.gov.uk/ukpga/1997/50/section/93, last accessed 2020/04/06.

National Police Chiefs Council, https://www.npcc.police.uk/documents/Policing%20Vision.pdf, last accessed 2019/09/29.

Office for National Statistics, https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/policeforceareadatatables, last accessed 2020/04.21.

Office for National Statistics, https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/homicideinenglandandwales/yearendingmarch2018#how-are-victims-and-suspects-related, last accessed 2020/06/04.

Owen, R.: Law Enforcement's Dilemma: Fighting 21st Century Encrypted Communications With 20th Century Legislation. Homeland Security Affairs (2018).

Pătraşcu, A. & Patriciu, V.V.: Beyond digital forensics - A cloud computing perspective over incident response and reporting. In. IEEE 8th International Symposium on Applied Computational Intelligence and Informatics, pp. 455-460 (2013).

Peters, M. A.: The information wars, fake news and the end of globalization. Educational Philosophy and Theory, 50 (13), 1161-1164 (2018).

Pollitt, M.: Six blind men from Indostan. In. Digital forensics research workshop (DFRWS) (2004).

Quick, D., Choo, K.K.R.: Impacts of increasing volume of digital forensic data: A survey and future research challenges. Digital Investigation 11(4), 273-294 (2014).

Raine, J.W. & Keasey, P.: From Police Authorities to Police and Crime Commissioners. International journal of emergency services, (2012).

Ramakrishnan, N., Butler, P., Muthiah, S., Self, N., Khandpur, R., Saraf, P., Wang, W., Cadena, J., Vullikanti, A., Korkmaz, G., Kuhlman, C.: August. 'Beating the news' with EMBERS: forecasting civil unrest using open source indicators. In. Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 1799-1808 (2014).

Robertson, A.: Policing by Consent: Some Practitioner Perceptions (Doctoral dissertation. University of Sunderland (2016).

Rogers, C. & Scally, E.J.: Police use of technology: insights from the literature. International Journal of Emergency Service, 7(2), 100-110 (2018).

Scheuerman, W.E.: Whistleblowing as civil disobedience: The case of Edward Snowden. Philosophy & Social Criticism 40(7), 609-628 (2014).

Segal, H.P.: Technopoly: The Surrender of Culture to Technology. The Organization of American Historians (1993).

Sentencing Council, https://www.sentencingcouncil.org.uk/the-magistrates-court-sentencing-guidelines/, last accessed 2020/04/22.

Shaw, D, https://www.bbc.co.uk/news/uk-44884113, last accessed 2019/10/21.

Shearing, C.D. & Stenning, P.C.: Private security: implications for social control. Social problems 30(5), 493-506 (1983).

Sheptycki, J.: Technopoly and Policing Practice. European Law Enforcement Research Bulletin (4 SCE), 133-139 (2019).

Sherman, L, Neyroud, P.W., Neyroud, E.: The Cambridge Crime Harm Index: Measuring Total Harm from Crime Based on Sentencing Guidelines. Policing 10 (3), 171-183 (2016).

Slessor, J, https://www.accenture.com/gb-en/insights/public-service/reimagining-police-workforce-future-vision, last accessed 2019/09/28.

Smith, T.: The “near miss” of Liam Allan: Critical problems in police disclosure, investigation culture, and the resourcing of criminal justice. Criminal Law Review (9) (2018).

Son, S., Jung, G., Jun, S.C.: An SLA-based cloud computing that facilitates resource allocation in the distributed data centers of a cloud provider. The Journal of Supercomputing 64 (2), 606-637 (2013).

Spinello, R.A.: Ethics in Cyberspace: Freedom, Rights, and Cybersecurity. Next-Generation Ethics Engineering a Better Society, 454 (2019).

Staniforth, A.: Police use of open source intelligence: The longer arm of law. In Open Source Intelligence Investigation, 21-31. Springer, Cham. (2016).

Taddeo, M. & Floridi, L.: Regulate artificial intelligence to avert cyber arms race. Nature 556 (7701), 296-298 (2018).

Taylor, M. Haggerty, J. Gresty, D. Hegarty, R.: Digital evidence in cloud computing systems. Computer, Law & Security Review 26 (3), 304-308 (2010).

Trenwith, P.M., Venter, H.S.: Digital forensic readiness in the cloud. In. Information Security for South Africa, 1-5. IEEE (2013).

Trottier, D.: Open source intelligence, social media and law enforcement: Visions, constraints and critiques. European Journal of Cultural Studies 18 (4-5), 530-547 (2015).

United Nations Office on Drugs and Crime, https://www.unodc.org/documents/organized crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf, last accessed 2019/11/01.

Van Baar, R.B., Van Beek, H.M.A., Van Eijk, E.J.: Digital Forensics as a Service: A game changer. Digital Investigation 11, 54-62 (2014).

Wall, D.S., Johnstone, J.: The industrialization of legal practice and the rise of the new electric lawyer: The impact of information technology upon legal practice in the UK. International Journal of the Sociology of Law 25(2), 95-116 (1997).

Waterhouse, J, https://www.bbc.co.uk/news/uk-46964659, last accessed 2019/12/20.

Williams, J.: Legal and ethical issues surrounding open source research for law enforcement purposes. In. ECSM 4th European Conference on Social Media. Academic Conferences and Publishing Limited (2017).

Woods, L.: Automated Number Plate Recognition: Data Retention and the Protection of Privacy in Public Places. Journal of Information Rights, Policy and Practice 2(1), 1-21 (2017).

Wright, S, http://eprints.leedsbeckett.ac.uk/2096/3/Watching%20Them%20Watching%20Us.pdf, last accessed 2019/12/20.

Yoannou C.J, https://www.prindlepost.org/2020/02/sensorvault-and-ring-private-sector-data-collection-meets-law-enforcement/, last accessed 2020/02/28.