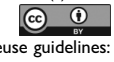
Check for updates

Original Research Article

THE INTERNATIONAL JOURNAL of EVIDENCE & PROOF

The International Journal of Evidence & Proof
1–19
© The Author(s) 2023

Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/13657127231171620
journals.sagepub.com/home/epj


Digital evidence in defence practice: Prevalence, challenges and expertise

Dana Wilson-Kovacs
University of Exeter, Exeter, UK

Rebecca Helm
University of Exeter, School of Law, Exeter, UK

Beth Growns
University of Canterbury, Christchurch, New Zealand

Lauren Redfern
King's College London, London, UK

Abstract

This article examines how criminal defence lawyers in the English adversarial system understand and use digital evidence (DE). Its first aim is to provide an empirical insight into their practices. Secondly, the article seeks to analyse the difficulties encountered by these professionals in accessing and working with DE—both those that they receive from the prosecution and those presented by the DE they need to defend their clients. Thirdly, the article discusses how criminal defence lawyers understand DE and its limitations and select relevant expert witnesses. Fourthly, it considers how the tensions discussed can be overcome. It is argued that while systemic issues outside the control of criminal defence lawyers are likely to impact the speed with which DE and witness expertise are secured, improving these professionals' digital literacy remains key to best representation and successful criminal justice outcomes.

Keywords

criminal defence teams, digital evidence, criminal investigation, prosecution teams, digital forensic expertise

Introduction

Digital devices provide information that helps track, interpret and contextualise the actions of individuals involved in criminal activities. The ubiquity of 'digital dust' and trace (Innes et al., 2021) offers both new

Corresponding author:
Dana Wilson-Kovacs, Department of Social and Political Sciences, Philosophy and Anthropology, University of Exeter, Amory Building, Rennes Drive, Exeter, EX4 4RJ, UK.
Email: m.d.wilson-kovacs@exeter.ac.uk

Correction (May 2023): Article updated to correctly list the grant information under Funding, which was mistakenly placed under Acknowledgements.

investigative opportunities and numerous challenges for criminal justice agencies. With 90 per cent of cases in England and Wales now containing a digital element (NPCC, 2020), fair criminal justice outcomes depend on dealing effectively with digital evidence[1] (DE) and identifying and addressing the dangers of mishandling, misinterpreting and manipulating it (Tully, 2020). Risks of ineffective practice are not confined to the digital forensic laboratory but are present throughout the journey of DE within the criminal justice system, as several recent cases illustrate.

The Post Office Scandal is perhaps the best known: between 2000–2014 over 900 postmasters were prosecuted, and the majority were convicted of theft, fraud and false accounting after shortfalls were flagged in their accounts by their accounting platform called Horizon. It has subsequently been recognised that many of these shortfalls were the result of faults in the Horizon system, rather than the postmasters' wrongdoing.[2] As the limitations of the Horizon system were largely unacknowledged and poorly understood during the initial litigation, the shortfalls were not attributed to these faults. In this case several factors contributed to the multiple miscarriages of justice (Moorhead et al., 2021): the unreliable evidence of an unpredictable computer system that judges, juries and lawyers failed to understand correctly, the Post Office's inability to provide proper disclosure (Marshall, 2020: 47), investigative failures and misleading witnesses.

Another example is the case of Danny Kay,[3] whose conviction for the rape of a 16-year-old was based on a complainant's testimony and Facebook messages from her mobile phone. It was only later when one of Kay's family members discovered how to retrieve messages between Kay and the complainant that had been deleted, that it became clear that the complainant had selectively deleted messages and given a misleading impression at trial. The conviction was quashed, but only after Kay had served four years in prison. Similarly, Jodie Rana's[4] conviction for arson was based on signal data from her mobile phone, which according to the prosecution's expert, placed her near the property she allegedly targeted. After serving more than two years in prison, Rana was acquitted when subsequent analyses of the home router at the property demonstrated that the device's coverage to Rana's phone was considerably wider than had been stipulated by the prosecution expert at the initial trial. This placed Rana further away from the incident and undermined the prosecution's case.

These cases illustrate the central role DE can play in miscarriages of justice when it is not handled effectively, and specifically when the DE used by the prosecution cannot be critiqued by defence lawyers. In the Post Office cases, the defence were unable to successfully identify flaws in the Horizon system; in the Kay case the defence could not identify and retrieve deleted Facebook messages, and in the Rana case, the defence could not demonstrate inadequacies in the cell site analysis presented by the prosecution's expert witness (and actually accepted conclusions of that witness as agreed facts). These examples are likely the tip of the iceberg in terms of injustices resulting from flaws in the use of DE. They show how deficient disclosure, a fragmented understanding of DE and a lack of comprehensive testing and analysis of digital devices and the information they carry, impact negatively criminal justice outcomes. They also illustrate the importance of having a well-trained cadre of legal professionals to prevent miscarriages of justice and ensure that convictions do not occur because of unreliable or inconclusive DE.

Knowing more about how DE is utilised in practice can help develop a more comprehensive understanding of how injustices in this area occur and assist in identifying systematic flaws in current

1. We define digital evidence as 'any information processed in numeric representation which supports or refutes a hypothesis about the state of artefacts or events of potential relevance and probative value for a criminal investigation' (cf. Stoykova, 2022). This can include data obtained from any digital device or online platform including (but not limited to) phones, computers, tablets, WiFi routers, cameras and gaming consoles, Internet of Things, connected vehicles and wireless sensors.
2. *Bates* v *Post Office* [2019] EWHC 3408 (QB); *Hamilton* v *Post Office* [2021] EWCA Crim 577.
3. See Evidence Based Justice Lab, *Danny Steven Kay*. https://evidencebasedjustice.exeter.ac.uk/case/danny-steven-kay/.
4. See Evidence Based Justice Lab, *Jodie Rana*. https://evidencebasedjustice.exeter.ac.uk/case/jodie-rana/.

approaches to DE. Many forensic practitioners and policy analyses have considered the evidential requirements of digital data. In addition, a rising number of socio-legal and criminological studies have discussed how DE is used by police and prosecution (e.g., Brookman et al., 2022; Daly, 2022; Wilson-Kovacs et al., 2022). This body of knowledge provides valuable insights but offers little information into the equally important work of criminal defence teams in an adversarial system. Topical analyses in this area remain scarce (e.g., Ramirez, 2022; Warren and Salehi, 2022), and rarely focus on the UK (e.g., Richardson et al., 2022).

To redress the balance, we concentrate here on the less documented experiences of criminal defence lawyers in the English criminal justice system, the challenges they encounter in responding to and utilising DE, and how these can be addressed. The aim of the article is four-fold: first, to provide an empirical insight into how DE is currently being used in criminal courts. Secondly, to present an up-to-date discussion of the difficulties criminal defence lawyers face in accessing and processing both the DE presented by the prosecution and the evidential information they require to defend their clients. The third aim is to examine how these professionals select and use digital expert witnesses, and how they reflect on their own understanding of DE and its limitations. The fourth aim is to explore how the tensions presented can be overcome. We argue that while systemic issues outside the control of criminal defence lawyers impact the speed with which DE is accessed and expertise secured, improving the lawyers' own digital literacy is key to ensuring they can represent adequately the interests of their clients. Our analysis contributes to the emerging field of critical forensic studies (Julian et al., 2021) and to socio-legal and criminological research on the use of DE in investigations, pre-trial and in-court proceedings (e.g., Brookman et al., 2022; Daly, 2022; Henseler and van Loenhout, 2018; Ramirez, 2022; Stoykova, 2021; Warren and Salehi, 2022; Wilson-Kovacs and Wilcox, 2022).

The paper is organised as follows: the **Background** section introduces the current socio-legal landscape within which criminal defence lawyers undertake their work in England. Drawing on three of the defining factors of the current situation, i.e., government resources for criminal defence work, the forensic market and disclosure guidelines—it offers a broader context for our analysis. The **Literature Overview** section examines the main topical issues related to the use of DE in the criminal justice system, as identified in the existing forensic and police practitioner and academic literature. The **Methodology** section prefaces our analysis with details of our research design and methods. The **Findings** section discusses the emergent themes, considering the challenges criminal defence lawyers face in accessing and scrutinising DE and recruiting expert witnesses, and their own understanding of DE and training needs. The **Discussion** and **Concluding Remarks** sections explore our findings in the context of existing debates and reflect on how the tensions presented can be addressed.

Background

Strains on the criminal justice system

The growing use of digital data for evidential purposes has led to an escalating demand for digital forensic analysis (e.g., Guttman et al., 2022; Richardson et al., 2022). This requires keeping up with the pace of technological change, including the growing data storage capacities and diversity of systems, and expensive infrastructural and workforce training investments that despite ongoing attempts to address these issues, exceed the current capabilities of criminal justice actors in England and Wales (e.g., House of Lords, 2018; Muir and Walcott, 2021; NPCC 2020) and elsewhere (e.g., Erlandsen, 2019; Henseler and Van Loenhout, 2018; Marshall, 2020; Ramirez, 2022; Stoykova, 2021). These developments also contribute to the challenges experienced by the criminal defence community.

Compared to other areas of the criminal justice system in England and Wales, the criminal defence community is small, with only 2,400 out of 17,000 practising barristers specialising in this field (Garside and Grimshaw, 2022). The profession has been affected by cuts in government funding for

criminal defence work, which has seen expenditure on criminal legal aid declining by 43 per cent in real terms from £1.2 billion in 2004/05 to £841 million in 2019/20 (Bellamy, 2021: 1.19). Post-pandemic, the reduction in budgets and the impact of COVID have left services on the brink of collapse (Bowcott, 2020). These measures have affected negatively both the lawyer-client relationship (Dehaghani and Newman, 2022) and the future of the criminal defence profession. They also lead to more pressure on defence lawyers to deal quickly with cases, which also often involve increasingly complex DE. Recent strikes by barristers specialising in criminal law highlight the scale of this issue (Davies, 2022). These tensions are important to note in the context of the British adversarial system, which relies on robust legal defence that is on equal footing with the prosecution ('equality of arms') (e.g., Bellamy, 2021: 1.34). In this system, the defence should have the same access and ability to utilise and critique all the evidence as the prosecution. Failing this, the principle of equality of arms is compromised, and the right to a fair trial is undermined. Central to this endeavour has been the forensic science support available to the defence and the effective disclosure of evidence from the police and prosecution to the defence.

Forensic expertise for the defence

The quality and delivery of forensic science in England and Wales have been deemed inadequate due to 'simultaneous budget cuts and reorganisation, together with exponential growth in the need for new services such as digital evidence' (House of Lords, 2018: 3). Following the dissolution of the Forensic Science Service in 2012, the forensic market in England and Wales has been fragmented and unstable. Three main firms (Eurofins, Cellmark and Key Forensics) have provided the bulk of the defence and prosecution evidential work for most types of forensic evidence (McCartney and Shorter, 2020). This excludes fingerprints, which are often analysed by specialist police personnel based in the forensic science support teams of police forces. Similarly, in some forces, most DE is extracted and analysed in-house by predominantly civilian police specialists working in digital forensic units. Over the last two decades, the impact of technological change led to the exponential growth in the diversity of sources and the volume of DE, the use of DE in court and a shortage of digital forensic expertise (NPCC, 2020; Richardson et al., 2022). Given the demand for DE, less complex analysis has typically been performed by police officers trained in basic extraction techniques of mobile phone data. Some forces outsource requests for digital forensic analysis to either one of the three main firms, or to other independent companies that specialise exclusively in DE. Many small practices also offer digital expertise for the defence; however, the size of this market is unknown as no figures are available.

Furthermore, providing forensic expertise for a defendant relies on the ability of the defence team to secure the legal aid funding necessary to commission expert service and the timeliness of their application. This process is subject to competitive bidding, with teams having to submit three expert quotes to the Legal Aid Authority (LAA), detailing the work required. However, the low expert payment rates and 'demobilising interactions with the LAA' (Welsh and Clarke, 2021: 468) have led defence lawyers and expert witnesses to query the quality of casework provided, to question the long-term sustainability of the criminal defence profession and to highlight the increase in the risk of miscarriages of justice (Bellamy, 2021; Dehaghani and Newman, 2022).

Current disclosure guidance

Failures to disclose key DE (and evidence more generally) have been said to bring the criminal justice system in England and Wales to a breaking point (Collie, 2018; Johnson and Smith, 2020). The 2022 Attorney General's Revised Guidelines on Disclosure and a Code of Practice, together with the 2018 Crown Prosecution Service (CPS) Guide to 'Reasonable Lines of Enquiry' and Communication Evidence, provide the framework for managing the disclosure obligations stipulated by the Criminal Procedure and Investigations Act 1996 and the codes issued under that act. They implement the

recommendations of the 2018 Review of the Efficiency and Effectiveness of Disclosure in the Criminal Justice System, which identified significant disclosure failings and called for a better approach to its management. To date, however, a key goal of the criminal justice system remains 'to establish an effective system of flexible, organic interaction to facilitate information sharing which is distinct from but supports the formal processes of disclosure and service of defence case statements' (2022: 9, 2B).

Central to this interaction is the selection of information and its timely communication between the police, prosecution and defence. While historically all digital devices were processed and analysed, the widespread use of digital devices by victims, witnesses and suspects, the diversity of devices and platforms, and massive storage capabilities mean that more cautious approaches are required for handling DE. The recent 2018 CPS Disclosure Guidelines acknowledged how a 'run-of-the-mill' investigation can generate tens of thousands of pages of data downloaded from multiple digital devices (House of Commons, 2018: para. 52–61), and advised that a careful selection of devices with potential evidential information is undertaken. However, this goal is still to be accomplished, as local guidance and practices vary across the 43 forces of England and Wales (McCartney and Shorter, 2020).

Moreover, the 2018 CPS Disclosure Guidelines advocate proportionate searches that consider cases individually and pursue all reasonable lines of inquiry, whether pointing towards or away from the suspect. Investigators are responsible for determining these depending on the circumstances of each case. However, as much of the topical literature reiterates (e.g., Anderson et al., 2021; Muir and Walcott, 2021) and the 2022 General Attorney's Revised Guidelines highlight, proportionate searches, reasonable lines of inquiry and timely disclosure remain challenging, due to difficulties in understanding the potential and limitations of DE, issues with formulating appropriate investigative strategies that identify DE in a methodologically rigorous manner and the embedded organisational cultures and practices of police and prosecution.

Literature overview of DE challenges

Home Office and police reports, forensic practitioner studies and academic scholarship (e.g., Collie, 2018; Holt et al., 2015; Muir and Walcott, 2021; Richardson et al. 2022; Tully, 2020) widely acknowledge how the pace and scale of technological change impact both forensic practitioners, who must acquire information forensically in very short timeframes, and the wider legal community, which 'must be prepared to deal with an increase of digital evidence in both volume and complexity' (Henseler and van Loenhout, 2018: 76). This section introduces briefly the key issues related to DE standards and requirements, use in court and gaps in training.

While DE should be subject to comprehensive reviewing (Casey, 2019; Guttman et al., 2022), and similar scientific rigour to that applied to other forms of forensic evidence (Collie, 2018; Tully, 2020), this remains problematic for law enforcement agencies. Likewise, establishing and maintaining standards in the digital field is particularly complex: the accreditation of digital forensic practices highlights the need for robust quality management systems (Page et al., 2019; Tully, 2020), as well as the ambiguities surrounding the ways in which digital (forensic) expertise is defined. For instance, the extraction and examination of data from mobile phones often take place outside the digital forensic units and are often performed by police officers with minimal training and little awareness of digital forensic principles (Collie, 2018; Wilson-Kovacs et al., 2022). As remits and limits of expertise become blurred, so do ownership and accountability, resulting in DE, especially from that from mobile devices, being contested in court (Anderson et al., 2021).

Socio-legal scholarship adds further insight into the challenges raised by the lack of quality assurance of DE in court, where old procedural guarantees that are unsuitable for assessing DE and the absence of reliability testing can result in inconsistencies and undermine the right to a fair trial (Henseler and van Loenhout, 2018). More broadly, unlike more established forensic techniques that have been subject to more scrutiny and fair trial guarantees, the lack of European minimum standards for DE has led to courts accepting this type of evidence without scientific validation of the methodology and tools used (Stoykova, 2021).

Legislative intervention, pre-trial reliability evaluation and formal verification of forensic procedures by the court are some of the measures proposed to address these limitations (Stoykova, 2021, 2022).

The use of DE has also created a digital divide between prosecution and defence in adversarial criminal justice systems (Ramirez, 2022), giving prosecutors and police more control over evidential data and better access to specialist expertise (Warren and Salehi, 2022). These power inequalities add to calls for closer collaboration between police, prosecution and defence and appropriate and timely disclosure (Anderson et al., 2021; Bellamy, 2021).

Overall, there is also the pressing need to embark on more targeted DE training for the judiciary. Erlandsen's analysis (2019) of how Norwegian prosecutors evaluate different types of DE illustrates the ways in which an inconsistent understanding of DE can lead to fallacies in the presentation and weighting of this type of evidence. Judges' and juries' lack of clarity on how digital devices and the software used to extract DE operate and their struggle to evaluate technical evidence must also be addressed (Anderson et al., 2021; Marshall, 2020). However, despite calls for reforming law schools' curricula by including more information about DE and the challenges in its collection, examination and chain of custody (Alva and Endicott-Popovsky, 2012), criminal defence lawyers continue to experience computer-literacy related difficulties. These concern both the understanding of digital forensic processes and the application of legal jurisdiction to the use of DE when such evidence is a key component of a case (Anderson et al., 2021).

Keeping up with technological change also extends to expert witnesses. Given the complexity of the digital field, Henseler and van Loenhout propose minimum training requirements of 'at least 3 years of relevant work experience at the level of an academic Master's Degree or at least 5 years at the level of an academic Bachelor's Degree, preferably in the field of technical IT' (2018: 580). Accordingly, expert witnesses should also 'demonstrably have interpreted and reported a minimum of 5 case reports in the preceding 5 years and have followed a minimum of 50 h of forensically relevant professional development (e.g., attending conferences, running or attending courses, publications)' (idem). In the UK, the Forensic Science Regulator's Codes of Practice and Conduct for Forensic Science Providers and Practitioners in the Criminal Justice System (2021) offer more general guidance for forensic personnel covering all disciplines. However, the Codes do not stipulate any requirements other than that for laboratory activities, staff must be ISO17025 standard compliant and for crime scenes, ISO17020 compliant. For some activities, including but not limited to the manual classification of indecent images of children, the recovery and replay of CCTV, and the extraction of data from cameras used at an incident scene, competency in the standard is not required. Moreover, the Codes have not covered thus far the activities of forensically untrained and often inexperienced police officers who have reportedly been used by the prosecution for presenting digital data in court (Collie, 2018). Below we explore the views of criminal defence lawyers about these issues and their own experiences of working with DE and the challenges they face. Before this, we briefly introduce our methodological framework.

Methodology

Our analysis draws on a multi-methods approach combining a survey with 70 solicitors and barristers who work in criminal defence in England, and 22 semi-structured interviews with 23 solicitors and barristers in this field.[5] Interview participants were self-selected from the survey respondents. Both data sets were collected between February and March 2022 and contained questions on how defence lawyers and their teams use DE, their knowledge of DE and their training needs. Survey findings provided a starting point for interviews, which explored in more detail participants' practices and perspectives on DE.

5. Note that participants were free to skip questions in the survey. Fifty-three participants answered all questions, and the remaining 17 participants answered a selection of questions. Where percentages or other quantitative data are reported in our analysis, the relevant sample size will be provided in cases where not all participants answered the question.

Survey description

Survey data was gathered through an online instrument hosted on the Qualtrics survey platform. A short summary of the issues examined is given below. Respondents also answered equivalent questions about feature-comparison evidence, which provided a helpful analytical contrast but is not discussed here. DE was defined as evidence obtained from online platforms and digital devices (including, but not limited to, mobile phones and tablets). Questions were free response unless noted otherwise.

Respondents were first asked about the type and presentation of DE they encountered, and the frequency with which they receive DE from the prosecution. Using a percentage scale from 0 ('used in none of my cases') to 100 ('used in all of my cases'), they were also asked about how often they used DE to defend their clients and how often their casework included other types of forensic evidence. Next, on a 6-point scale from 'always' or 'almost always' to 'never' or 'almost never', respondents were asked how often they challenged DE, how they critique or scrutinise it, how conclusive they typically considered DE to be, and the difficulties they face evaluating the DE presented by the prosecution.

The second part of the survey asked respondents about how they access and select digital experts and evaluate their expertise. Respondents were also required to comment on whether jurors had a good understanding of DE. The third part of the survey asked respondents whether they considered themselves to have a good knowledge of DE, the training they received and the additional guidance they would benefit from. To conclude the survey, respondents were asked to provide some demographic data. All responses were anonymous.

Survey sample characteristics

Respondents worked in criminal defence as solicitors (including duty solicitors) and barristers and practised in both Crown and Magistrates' Courts across England. Fifty-three of the 70 respondents provided their age, and 54 included their years of experience: these were aged between 25–67 ($M = 45.47$, $SD = 10.72$) and had between 0.5 and 42 years of legal experience ($M = 19.14$, $SD = 10.29$). Respondents had experience with case types such as homicides, terrorism, organised crime (including multi-defendant and county lines cases and money laundering conspiracies), serious sexual offences (including rape and the possession, distribution and making of indecent images of children), serious violence, robbery, firearms, drink driving, road traffic accidents, shoplifting, fraud, and hunting, shooting and fishing offences.

Data analysis

Answers to forced-choice questions were analysed quantitatively. Thematic analysis (Braun and Clarke, 2006) was used to examine survey responses to open-ended questions. An iterative inductive approach was adopted to identify the main concerns raised in the survey responses and fine-tune the interview questions, which further probed participants' experiences of DE. In the design of the survey questions a distinction was drawn between how the defence worked with DE received from the prosecution and how the defence accessed and used DE for their cases. Because the analysis of the survey responses suggests defence teams encounter similar challenges in both these aspects of their practice, the interview questions focused on exploring further these difficulties. The 22 one-hour interviews were recorded, transcribed and anonymized. Each transcript was coded independently by two of the authors. These codes were then compared for accuracy, with the differences between coders reviewed in each case to establish consensus. Constant comparison between the interview and survey data was undertaken to ensure that the saturated themes reflected reliably participants' views, which are presented below.[6]

6. In the data discussion below, interview responses are identified by I+number (e.g., I04) and survey responses by S+number (e.g., S21).

Findings

The prevalence of different types of forensic evidence and the use of DE

When respondents were asked to rate the use of different types of evidence on a scale from 0 (never or almost never) to 100 (always or almost always), survey data highlight the importance of DE in current practice.

Evidence from a mobile telephone ($M_{\text{prosecution}} = 49.87$, $SD = 26.82$, $M_{\text{defence}} = 31.17$, $SD = 22.03$), evidence from a computer ($M_{\text{prosecution}} = 30.19$, $SD = 22.87$, $M_{\text{defence}} = 18.86$, $SD = 18.83$) and evidence from an online platform ($M_{\text{prosecution}} = 31.99$, $SD = 24.82$, $M_{\text{defence}} = 20.19$, $SD = 21.79$) were, on average, rated as the top three most commonly used types of forensic evidence by the defence (see Figure 1), and as three of the top four most commonly used types of forensic evidence by the prosecution, alongside DNA evidence ($M_{\text{prosecution}} = 36.76$, $SD = 27.67$, $M_{\text{defence}} = 9.84$, $SD = 15.38$) (see Figure 2).

Types of DE used by the prosecution. The prosecution was reported to use several DE sources, including mobile phones, tablets, PCs, (external) hard drives, USB sticks, discs and other fixed storage items, doorbell cameras, webcams, dash cams, GPS and trackers. Many respondents identified mobile phone data as a typical source of DE used by the prosecution, a finding corroborated by Richardson et al.'s recent study (2022). Fifty-three respondents noted data from mobile phones as being typical digital evidence used by the prosecution, while the remaining 12 respondents only referenced data from computers, other devices or from social media platforms.

Message history information, exchanges on platforms such as WhatsApp, Facebook Messenger and Snapchat, and traditional SMS texting were all frequently cited types of DE used by the prosecution, and DE provided was described as relevant for many offences:

> Message downloads and cell site evidence from mobile phones…are nearly always used in prosecuting drugs cases but can also be found in lots of other types of cases, harassment, malicious communications, breaches of restraining orders, assaults or murder for location, or messages to help with motive. (S21)

Twenty-six respondents noted cell site evidence tracking the location of mobile phones as being typically used by the prosecution, with several noting how this type of DE is often important in cases involving drug-related offences.

Respondents reported they received DE from the prosecution in several formats: usually digitally as specialist reports, PDF documents, Excel spreadsheets and screengrabs. DE could be accessed through secure, virtual hosting platforms such as the Crown Court Digital Case System, evidence.com and Egress. Around a quarter of respondents noted that sometimes DE was sent on a memory stick or disc.

Types of DE used by the defence. Fifty-seven respondents noted specific types of DE they typically use in their defence work, including cell site evidence and message data—such as screenshots of text message exchanges in SMS, Facebook and WhatsApp chat history. There was little systematic breakdown of DE sources in the survey responses. The aggregate list includes generic mentions of 'material from a phone', cell site data, PDF files, images and videos, CCTV, Excel spreadsheets, Google Maps and call log history. Respondents explained that occasionally they used the same messages as the prosecution, but refuted the prosecution's interpretation by reframing the content of the messages, elucidating their context and providing additional information:

> Message data [may] show that the 'offending contact' does not amount to harassment or stalking when viewed in context. For example, a threatening or abusive message may not amount to stalking when it forms part of an ongoing and two-way dispute between the parties. (S28)

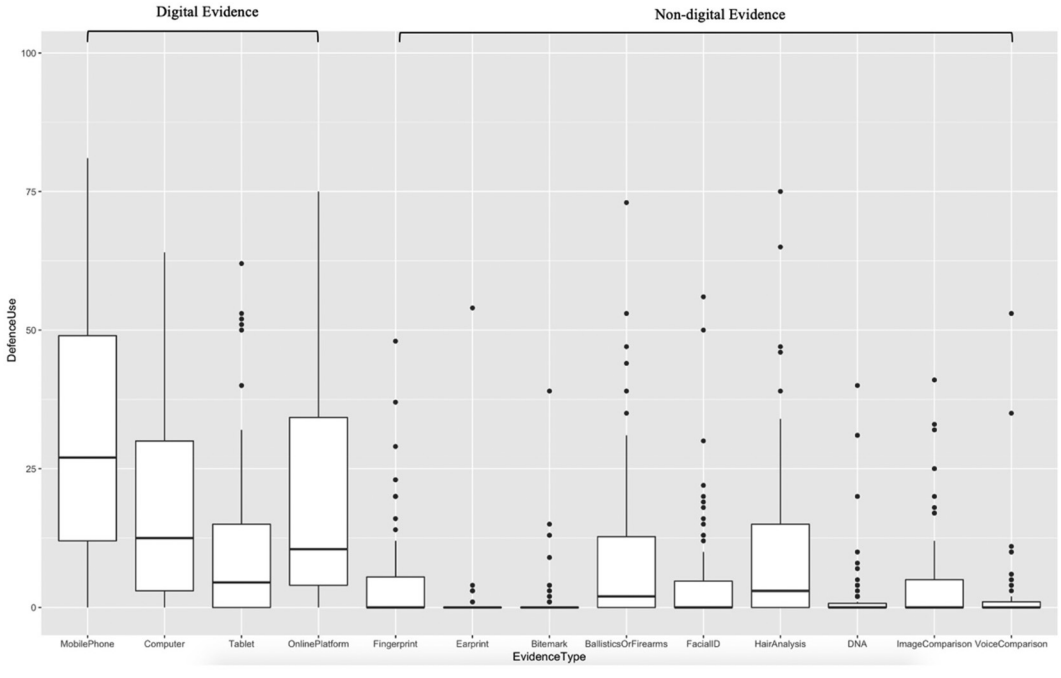


Figure 1. Box plots showing survey responses as to the percentage of defence cases where different types of evidence are used (based on each respondent's case work). Answers were on a scale from 0 ('never' or 'almost never') to 100 ('always' or 'almost always').

Challenges addressing and using DE

Volume, formats and presentation. Respondents noted how even 1GB of data produces unmanageable amounts of evidence to review:

> 1 GB of data is about 900,000 pages of text messages, 300 photos, 120,000 documents…when you] have between 64 GB to 2 TB of data, it takes a long time to work through the data. (S34)

They also remarked on the limited amount of time available to scrutinise the evidence presented by the prosecution: 'The sheer vast amounts of data [mean] you essentially have to rely upon the conclusions drawn at the end' (S73). This illustrates that defence teams can feel unable to examine all the evidence presented by the prosecution and indicates that sometimes they rely on the summaries provided by the prosecution. The inability to undertake independent checks to verify the accuracy of this evidence is one instance of the disparity of arms between the prosecution and the defence (Edmond et al., 2018). Affecting the extent and quality of the support defence lawyers provide to their clients, this can also result in omitting important details that can lead to miscarriages of justice.

Respondents criticised the format and presentation of DE received, remarking how the prosecution 'prints off schedules in the smallest font possible to cut down on page count' (I04) and how 'messages are just dumped in masses of pages along with call logs' (S21). Using terms such as 'dumped' suggest there can be little order, continuity and structure to how the prosecution presents DE. Adding to the volume of data our respondents were called to review, the often-inaccessible format in which data was offered was a major challenge. Finding the relevant evidential information manually was described as time-consuming and the DE presented by the prosecution reported as 'difficult to navigate and laborious

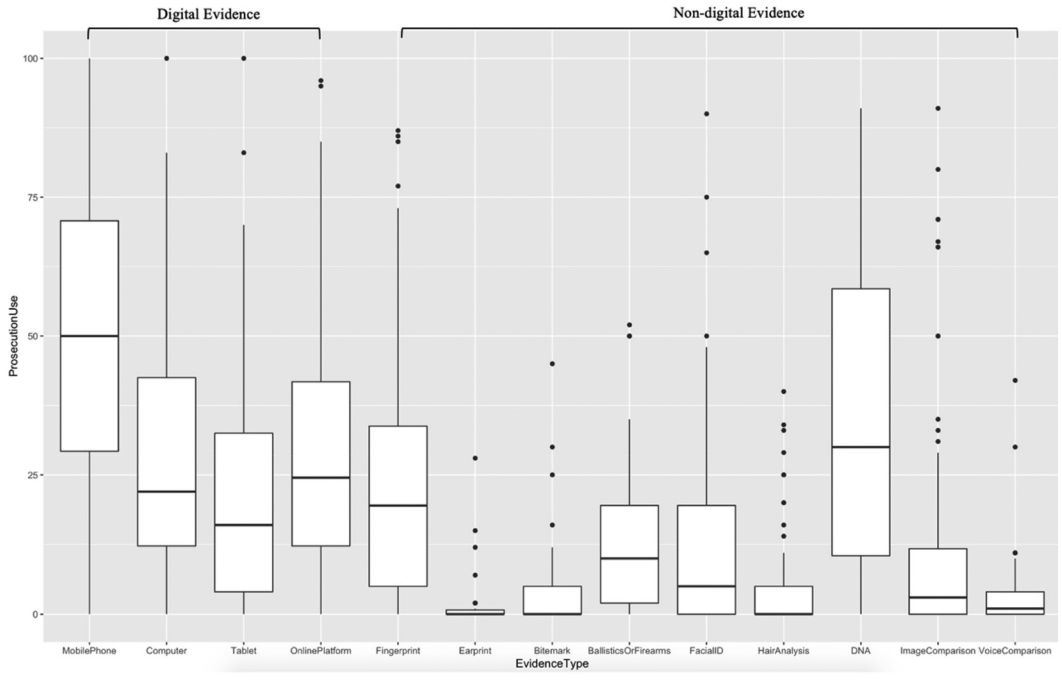


Figure 2. Box plots showing survey responses as to the percentage of prosecution cases where different types of evidence are used (based on the casework of the respondent). Answers were on a scale from 0 ('never' or 'almost never') to 100 ('always' or 'almost always').

to decipher' (I22). Some respondents described 'data dumps' (I07, I11, I19) as a prosecution tactic to slow down the progress of already overstretched defence teams, working with limited resources and tight schedules. Whilst the prosecution may not be at fault for presenting DE in this manner, establishing commonly agreed standard formats for increased accessibility is needed.

Funding, timing, access and disclosure. Many respondents identified challenges with funding, timing, access to DE and disclosure. Forty respondents indicated that the largest challenge was gaining access to data or the ability to use the data in the format provided, and 26 respondents noted difficulties processing and understanding large quantities of data in the context of a case. Twenty-one respondents reported that the sheer volume of data often made available is overwhelming and difficult to process. Others indicated additional challenges, including funding and cost ($n = 19$), being given access to data in a timely manner ($n = 20$), access to knowledgeable experts ($n = 9$) and disclosure ($n = 8$).

Echoing the findings of the Attorney General's Office Annual Review of Disclosure (2022) and Sir Christopher Bellamy's recent Review (2021), respondents discussed the lack of timely access to data as another deliberate prosecution strategy to restrict both the legal aid funding stream and the capabilities of the defence: 'They sit on it as long as possible to avoid triggering legal aid payments or increase payments to prosecution counsel' (S45). Consequently, 'sometimes such evidence arrives literally days before a trial giving no opportunity to obtain an independent evaluation of that evidence' (S53). As mentioned above, when defence teams did not have enough time to apply for legal aid and/or the in-house capacity to examine the evidence in the manner required, had to rely on the evidence summaries provided by the prosecution. 'Cherry picking' (Collie, 2018), a term used by some respondents to describe how police do not supply all the relevant material, omit details from the information they hold, or miss evidence altogether, was also reported.

Investigative material can be either relied upon at trial or gathered during the police investigation but not used or disclosed to the defence (McCartney and Shorter, 2020). Respondents also noted difficulties when attempting to access DE for the defendants and the problems of establishing contact and visiting the police forces where copies of the digital data requested were held. Due to the tight framework of obtaining legal aid, some noted the short time provided to secure independent experts for the analysis of the DE offered by the prosecution. They also remarked that even when defence expert witnesses were secured, access to other relevant data held by the police depended largely on the goodwill of the prosecution and would typically occur too late to be able to undertake any meaningful analysis. Finally, many participants noted how given the rather haphazard way in which police forces approached the alteration of unnecessary evidential information, what DE was made available to defence teams often lacked detail and context or was so heavily redacted that it was 'impossible to follow' (I21), which in turn affected its understanding and interpretation.

Using DE. The challenges presented about how DE is used to prepare one's defence were similar to those encountered when the defence received DE from the prosecution. Here, the lack of cooperation from the police when asked to provide access to digital data was the most significant for 30 per cent of respondents. Nineteen per cent of respondents noted the volume of data and the format in which the data was presented, and 17 per cent highlighted the time taken to access and identify the relevant information:

> The biggest challenge is the quantity of evidence from digital services (hence we typically instruct an expert). If the prosecution serves the raw data to us (usually requested) we are faced with a large quantity of data, a lot of it irrelevant and combing through everything on the device can be challenging and time-consuming. (S23)

Further difficulties were noted about gaining the cooperation of social media companies—especially those based overseas—to access the information needed, and bypassing two-factor authentication:

> It is very hard to obtain data from social media companies. They don't easily cooperate, particularly if based overseas. If the prosecution have not examined seized phones, then accessing social media accounts that require two-factor authentication is very, very difficult. Generally, you have to instruct experts to access social media accounts because of the inherent risks of accessing accounts from your desktop. (S54)

This fragment also suggests that defence lawyers undertake the examination of evidential information themselves, without the use of a digital expert, a point to which we shall return shortly.

Challenging the prosecution expert's conclusions and choosing defence experts

Most survey respondents said they challenged conclusions from a prosecution expert 'frequently' (20 per cent), 'very frequently' (20 per cent), 'always' or 'almost always' (6 per cent). Forty-seven per cent said they 'sometimes' did so, and 4 per cent did so 'very infrequently'.[7] For some, independent expertise was sought only when the defence team lacked the appropriate skills to undertake the analysis—e.g., one respondent explained that they would 'instruct an expert where it is too complicated for me' (S54). While the more technical aspects of the evidence were likely to require an expert's input, the interpretation of messages was not seen as such.

Some respondents noted how they manually checked the DE presented by the prosecution because details could be 'missed'. Others highlighted how they triangulate the evidential information they receive from the prosecution before considering whether expert advice is needed. This point was

7. This question was answered by 66 respondents.

elaborated in interviews, where participants discussed the extensive work they undertake before deciding to seek independent expert assistance:

> If a telephone report, for example a schedule, has been produced detailing contact between defendants, I check it against raw call data for anomalies and against phone downloads to verify content of messages which might assist with interpretation. (I07)

Decisions regarding the need for an independent expert were contextually dependent. The most important factors were the client's instruction (i.e., whether they accept the evidence or not) and the type of crime under investigation. Some participants mentioned querying all evidence, regardless of its type:

> I would normally assess a particular piece of evidence in full. For instance, if I am served with a forensic report alleging Drug Driving, I would always check the dates of the report and then when the analysis took place. This should be compared with the date of the allegation. (S27)

Some forms of DE were said to be harder to contest than others (e.g., IIOC or cell site analysis), because of their perceived factual status. Factual information (such as the location of a mobile phone at a given time) was more readily accepted as absolute and difficult to argue against than information from text messages, which was seen as easier to pull apart, interpret and entextualise (Daly, 2022). Most participants would rarely challenge such factual information, focusing instead on the content of messages and the interpretation possibilities this offered. As messages were often presented to the defence outside their wider context, further analysis and reframing seemed to be both possible and preferred, as one interview participant explained:

> It really depends on context. Interpretation of meanings of messages and communications, especially in drugs cases [for example] is open to challenge. Cell site analysis is less easily challenged because generally the limitations of the evidence are accepted by the prosecution expert. (I12)

Respondents remarked on the compelling nature of scientific evidence on juries and the power and influence of prosecution experts: 'Courts are often persuaded by prosecution experts unless defence experts are instructed to rebut their opinions' (S64). This quote also prefaces the task of the defence expert, i.e., being able to challenge successfully the evidence presented by the prosecution's expert and change the legal narrative. An additional task is to present the information in an accessible manner, as:

> Some jurors will be tech savvy and understand quickly, others may not and it can be difficult for them to grasp matters which they have no experience of. Important to understand that there may still be people on juries who don't have smart phones and are not familiar with general digital technology. (S42)

In the context of DE, 41 respondents sought to secure experts who had assisted them in similar cases and 'did a good job' (I10), or who were recommended by colleagues. Nineteen respondents chose experts using available in-house databases and independent registers. Twenty-nine respondents noted the importance of checking experts' CVs and credentials:

> I check within the firm for who is recommended. I go to experts I'm familiar with or who counsel recommends based on prior experience, I will check the credentials of the prosecution expert and ensure the expert I instruct has appropriate experience on their CV to be able to challenge with authority the other expert. (S42)

Availability, time and cost also mattered: using a 'tried and tested' (I2) expert who is available and can complete the assignment to a high standard and within the time and legal aid financial parameters was described as the 'ideal scenario' (I5):

> We tend to instruct the same small number of experts in every case. This is because once we have found an expert who is suitably qualified, easy to instruct, helpful and cost effective, you don't want to have to search elsewhere. (S28)

The decision to challenge a prosecution expert was typically linked to the likelihood of a successful outcome and the expert's credibility. On occasions, the interpretations provided by prosecution experts were not seen as conclusive under any circumstances. Furthermore, most respondents took issue with the experts used by the prosecution: 'Typically, the "experts" are experienced police officers. Courts/juries tend to find them persuasive' (S17). The use of quotation marks for 'expert' here illustrates the questionable status of these witnesses. The fragment also suggests that juries are unlikely to distinguish between the quality of expertise such officers provide and accept the evidence as conclusive. Many respondents also noted how the conclusiveness of an expert's opinion in court depends on their impact on the jury, rather than the accuracy of their analysis.

The likelihood of the defence accepting the prosecution experts' interpretation of DE as conclusive was linked to their qualifications: 'If a proper expert generally no problem. If say police on mobile phone download as an example I have to say I am often sceptical' (S43). Questioning the qualifications and status of prosecution experts was presented as typical of the approach used by the defence to clarify their expert status.

Understanding DE and training requirements

When discussing the possible mishandling and misunderstanding of DE and reporting on their own understanding of how DE was obtained and analysed, participants' responses varied greatly: 5 said they had no technical competence, 12 had limited understanding and 41 had some knowledge or described what they typically understood DE to be. Only one respondent reported a 'fairly good' understanding of DE. A typical explanation of the extraction of DE was:

> The police seize devices, they send the devices to a secure establishment and the devices are interrogated using police approved software. Social media accounts seem to be obtained through sterile means but I'm not sure exactly how, that's why we use experts! (S54)

Some responses to the comprehension questions indicate unease and a slightly defensive stance. For example, respondents explained that 'It's what is recovered that is important to me, not how' (S7) and 'I do not (know), nor necessarily need to know how (technology) works. I need to understand HOW that evidence assists the prosecution or helps the defence' (S24).

Others commented how screenshots provide an easy understanding of DE: 'When it's a screenshot clearly we know how that's done but beyond that no understanding' (S12). Here, the reference to 'how that is done' does not suggest insight into the evidential limitations of screengrabs, but simply the act of capturing the information on the screen, akin to that of taking a photograph. The few who reported possessing extensive knowledge, usually described the mechanisms of procuring DE:

> (Obtaining digital evidence from online platforms) is largely initially intersected with the assistance of Internet service providers who send material flagged to them to specialised teams, whether that be sex offences, terrorism or drugs and...that team then disseminates information to local police forces who can conduct more detailed enquiries dependent on urgency size, scale, etc. (S25)

The limitations of DE were discussed by only one respondent:

> There are different ways of accessing information and this can sometimes impact the result. E.g., different software could impact on how much is recovered. It's regularly obtained by police officers with limited training and digital experts will often be able to comment on whether the report is likely to be an accurate picture and can sometimes obtain additional information e.g., deleted material not seen initially. The parameters are also important and can change results e.g., a download or a full system dump. (S42)

Despite the lack of familiarity with forensic processes, responses displayed awareness of how DE could be corrupted:

> In low level crime officers play around with phones/devices with complainants and risk altering systems data or worse. In CID level work they properly image the device so they freeze it as a moment in time and cannot corrupt it. There is always one unaltered copy and then a working copy just in case something is lost or damaged. (S45)

However, thirty-six survey respondents indicated they had received no training in understanding and critiquing DE. Only 23 respondents reported receiving some training. Its type and frequency varied from attending 'the occasional webinar' to being not officially accredited and sporadic (received once, occasionally, or simply 'over the years', for instance, during their bar vocational course). Most training was part of continuing professional development in the workplace, or acquired by attending various events:

> I have attended seminars relating to the analysis of mobile phone evidence and how best to challenge call/message data. These seminars were hosted by lawyers though, not by forensic experts. (S28)

Occasionally the forensic science providers used by the defence teams offered training on analysing computer and mobile phone evidence or challenging cell site evidence. Some respondents reported self-teaching through podcasts and other online resources, reading topical articles and observing and asking experts: 'No formal training, it is simply what has been picked up over the years from discussions with experts and general geek knowledge about devices' (S5).

Content-wise, respondents expressed an interest in several areas: how digital experts achieve their status, how competencies are assessed, how DE is secured, how the software used to extract and interrogate DE works, how DE can be best presented to judges and juries, understanding cell site analysis and the data collection, analysis and limitations of DE, how platforms such as Facebook, Snapchat and WhatsApp work, how IP addresses can be used to identify suspects, and how to deal with Encrochat phones. This list illustrates the gaps in the current knowledge of DE that the defence lawyers we surveyed and interviewed have, and the wide range of information required to improve their understanding of DE.

Discussion

First, and most clearly, our findings illustrate the significance of DE in the current criminal justice system, complementing other recent studies regarding the scale of its use (e.g., Richardson et al., 2022). Our data confirms that DE is used more often than non-DE by both the prosecution and the defence. The average estimates of respondents' own caseload indicate that evidence from mobile phones is the most frequent type of DE used by the prosecution (in approximately 50 per cent of cases) and defence (in more than 25 per cent of cases). These estimates both support findings elsewhere (e.g., Richardson et al., 2022), and reinforce that the key to the appropriate administration of justice is ensuring that DE is handled correctly.

Our results also highlight flaws in how DE is used and critiqued. Similar to studies on US public defenders (e.g., Warren and Salehi, 2022), they suggest that the ability of criminal defence professionals

to access DE is restricted by the structure of the criminal justice system where police forces and the prosecution have more control over the evidential information than the defence teams. A lack of timely access and funding to interrogate the DE presented by the prosecution, and a fragmented understanding of DE limitations, are also reflected in our data. Compounding these issues is continued poor communication between criminal justice agencies (Bellamy, 2021; McCartney and Shorter, 2020; Tully, 2020).

One of the risks in the collection, analysis and reporting of DE resides in perceiving it as factual, which in turn makes interrogating it more difficult (Casey, 2019; Holt et al., 2015). Our findings highlight how the factual status attributed to some types of DE is rarely seen as worthy of scrutiny. They further suggest that the software, hardware and systems used to produce DE as factual are seldom scrutinised. As juries focus on the meanings extracted from evidence and communicated by adversarial parties in court, rather than the evidence itself (Edmond et al., 2020), and their decision-making process is based on narratives that clarify and reduce evidential ambiguities, it is important to acknowledge the limitations of DE, including those related to evidence accepted as factual and rarely, if ever, questioned.

Far from speaking for itself, evidence requires context, interpretation and sense-making (Kruse, 2016). Potentially confusing and contradictory evidence is typically embedded into legal narratives that give it credibility and help establish 'which party is telling the more plausible story' (Jasanoff, 2006: 329). Both prosecution and defence teams use such narratives to connect (or disconnect) people and their actions to (or from) crimes (Kruse, 2016). Digital trace is a key resource to this storytelling, primarily by helping to construct a 'plausible chronology' (Innes, 2002: 682) to account for events, actors and actions and reinforce the strength and authority of prosecutorial claims (Brookman et al., 2022). In contrast, for the defence, the storytelling centres on disputing the prosecution's findings. Our findings illustrate how the use of DE is restricted by limited or late access to evidential information, and the tight turnaround times to secure legal aid funding and choose and instruct independent experts. It is also circumscribed by the capacity to reconcile some of the issues raised by the volume, format and presentation of DE. In this context, being able to instruct experts correctly in the first place is essential. Our data, however, suggests this is not always the case.

Digital data can be manipulated to construct a particular narrative: in sexual misconduct cases, for instance, digital communications data from social media and mobile phone exchanges can be used in legal narratives to undermine the credibility of a survivor's moral character (Daly, 2022). Emojis, for instance, are often a point of contention, with one single character having the capacity to derail a case due to its multiple possible interpretive meanings. Warren and Salehi's (2022) analysis of public prosecutors recounting arguments over the meaning of emojis and slang used by defendants in their social media accounts, illustrates this in their description of the extensive debate about how the 100 per cent emoji coupled with a gun emoji could serve as sufficient evidence to confirm that a client was carrying a weapon without a permit, or whether the use of both emojis simply conveyed emphasis.

More generally, understanding how DE is assessed, analysed and presented in court is key, as this will affect how judges and juries will weigh its importance (Anderson et al., 2021). Clarity and transparency are needed around data collection and analysis, to reassure courts that due process has been observed. Given that defence teams usually receive only tailored reports (PDF documents or Excel spreadsheets) rather than the raw data and case files created during the early stages of an investigation, such clarity and transparency are particularly important. As Anderson et al. (2021) note and our findings confirm, defence lawyers are invariably tasked with concluding such reports that may not capture all the relevant data they need to draw upon in their defence strategy. Equally, analysing raw data is difficult and often requires specific and costly expertise and tailored DE training that is rarely covered by legal aid (Bellamy, 2021).

Concluding remarks

This article has examined how the increased use of DE in criminal proceedings generates several tensions and disadvantages for criminal defence lawyers in England and Wales, often encountered in accessing,

analysing and presenting such evidence. Our findings have some limitations. First, our sample represented only a small proportion of those with experience in legal defence and thus may not be completely representative. The sample may have also been skewed in favour of defence lawyers with an interest in this area. Second, our data is dependent on honest responses from survey respondents and interview participants. Although these limitations must be acknowledged, clear themes, that are likely to be important in practice more widely, emerge from our data (including the survey, where anonymity is likely to have encouraged transparent responding).

The amount, complexity and reliability of data have been noted as major risk factors in the use of DE (e.g., Casey, 2019; Stoykova, 2021; Tully, 2020; Warren and Salehi, 2022). Focusing on the experiences of criminal defence lawyers, our analysis further illustrates how DE is used, the delays in accesing legal aid, issues around disclosure, and decisions regarding experts. It highlights additional issues around the format and presentation of DE received from the prosecution and calls for streamlining these elements of the process. Some of the concerns raised by our participants are historical, systemic and pertain to most, if not all, types of forensic evidence. However, our findings suggest that the volume and diversity of DE escalate these tensions, postpone access to DE and increase turnaround times for the analysis of DE presented by the prosecution and sought by the defence. Additionally, difficulties in securing legal aid and the input of expert witnesses impact the thoroughness of the defence's presentation (Welsh and Clarke, 2021).

Our findings highlight the tendency to regard DE as factual, accessible and within our participants' analytical abilities. Both survey and interview data indicate that before choosing experts, and sometimes instead of doing so, some criminal defence lawyers attempt to analyse the data themselves. While this can happen because of the volume of data received from prosecution and the short time in which defence lawyers must prepare a response and secure legal aid funding, the limited amount of that funding and the independent expertise it can offer, the risk of omitting relevant evidential information in doing so is heightened. Given the absence of systematic training, this confidence is disconcerting: in line with other findings (e.g., Alva and Endicott-Popovsky, 2012; Erlandsen, 2019), it reinforces the widespread need to raise the levels of understanding of DE by all criminal justice actors, in terms of how DE is gathered and when and how it may be challenged.

Acknowledgements

We wish to thank our participants for their time and to our reviewers for their suggestions. The research data supporting this publication are not publicly available due to ethical and legal concerns. The survey instrument is available at https://doi.org/10.24378/exe.4624.

Declaration of conflicting interests

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

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: The support of the Economic and Social Research Council (Research Grant ES/R00742X/1) and Policy Support Fund at Policy@Exeter are gratefully acknowledged.

ORCID iDs

Dana Wilson-Kovacs https://orcid.org/0000-0001-5861-3617
Rebecca Helm https://orcid.org/0000-0003-1429-3847

References

Attorney General's Office. Annual Review of Disclosure. May 2022. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1078195/Annual_Disclosure_Review_Publication_Copy.pdf (accessed 27 September 2022).

Alva A and Endicott-Popovsky B (2012) Digital evidence education in schools of law. *The Journal of Digital Evidence, Security and Law* 7(2): 75–88.

Anderson P, Sampson D and Gilroy S (2021) Digital investigations: Relevance and confidence in disclosure. *ERA Forum. Journal of the Academy of European Law.* 22: 587–599.

Bellamy C (2021) Independent review of criminal legal aid: final report. Home Office. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1041117/clar-independent-review-report-2021.pdf (accessed 15 November 2022).

Bowcott O (2020) Legal aid services are on brink of collapse, lawyers tell MPs. The Guardian. 29 October. Available at: www.theguardian.com/law/2020/oct/29/legal-aid-services-brink-collapse-lawyers-tell-mps-justice (accessed 5 October 2022).

Braun V and Clarke V (2006) Using thematic analysis in psychology. *Qualitative Research in Psychology* 3(2): 77–101.

Brookman F, Jones H, Williams R, et al. (2022) Crafting credible homicide narratives: Forensic technoscience in contemporary criminal investigations. *Deviant Behavior* 43(3): 340–366.

Casey E (2019) The chequered past and risky future of digital forensics. *Australian Journal of Forensic Sciences* 51(6): 649–664.

Collie J (2018) Digital forensic evidence—flaws in the criminal justice system. *Forensic Science International* 289*:* 154–155.

Crown Prosecution Service (2018) Disclosure, guidelines to reasonable lines of inquiry and communication evidence. Available at: www.cps.gov.uk/legal-guidance/disclosure-guide-reasonable-lines-enquiry-and-communications-evidence (accessed 27 September 2022).

Daly E (2022) Making new meanings: The entextualisation of digital communications evidence in English sexual offences trials. *Crime, Media, Culture* 18(4): 578–596.

Davies C (2022) Criminal barristers vote to go on strike in row over legal aid. The Guardian. 20 June. Available at: www.theguardian.com/law/2022/jun/20/criminal-barristers-vote-strike-legal-aid-england-wales-crown-courts (accessed 5 October 2022).

Dehaghani R and Newman D (2022) Criminal legal aid and access to justice: An empirical account of a reduction in resilience. *International Journal of the Legal Profession* 29(1): 33–52.

Edmond G, Carr S and Piasecki (2018) Science friction: Streamlined forensic reporting, reliability and justice. *Oxford Journal of Legal Studies* 38(4): 764–792.

Edmond G, Cunliffe E and Hamer D (2020) Fingerprint comparison and adversarialism: The scientific and historical evidence. *The Modern Law Review* 83(6): 1287–1327.

Erlandsen TE (2019) Fallacies when evaluating digital evidence among prosecutors in the Norwegian police service (Masters Thesis, NTNU).

Forensic Science Regulator (2021) *Forensic Science Providers: Code of Conduct.* London: Home Office. Available at: www.gov.uk/government/publications/forensic-science-providers-codes-of-practice-and-conduct-2021-issue-7/forensic-science-providers-codes-of-practice-and-conduct-2021-issue-7-accessible (accessed 1 September 2022).

Garside R and Grimshaw R (2022) Criminal justice systems in the UK. Centre for Crime and Justice Studies. Available at: www.crimeandjustice.org.uk/sites/crimeandjustice.org.uk/files/Criminal%

20justice%20systems%20in%20the%20UK%2C%20August%202022.pdf (accessed 1 September 2022).

Guttman B, Laamanen MT, Russell C, et al. (2022) Results from a black-box study for digital forensic examiners. National Institute of Standards and Technology. NISTIR 8412. Available at: https://doi.org/10.6028/NIST.IR.8412 (accessed 1 September 2022).

Henseler H and van Loenhout S (2018) Educating judges, prosecutors and lawyers in the use of digital forensic experts. *Digital Investigation* 24: S76–S82.

Holt TJ, Bossler AM and Seigfried-Spellar KC (2015) *Cybercrime and Digital Forensics.* London: Routledge.

House of Commons (2018) *11th Report of the Justice Select Committee, 'Disclosure of Evidence in Criminal Cases'. HC859*. London: The Stationery Office.

House of Lords (2018) Forensic science and the criminal justice system: A blueprint for change. Science and Technology Select Committee 3rd Report of Session 2017-19 HL Paper 333.

Innes M (2002) The 'process structures' of police homicide investigations. *British Journal of Criminology* 42(4): 669–688.

Innes M, Brookman F and Jones H (2021) 'Mosaicking': Cross construction, sense-making and methods of police investigation. *Policing: An International Journal* 44(4): 708–721.

Jasanoff S (2006) Just evidence: The limits of science in the legal process. *The Journal of Law, Medicine and Ethics* 34(2): 328–341.

Johnson E and Smith T (2020) *The Law of Disclosure: A Perennial Problem in Criminal Justice*. London: Routledge.

Julian R, Howes L and White R (2021) *Critical Forensic Studies*. London: Routledge.

Kruse C (2016) *The Social Life of Forensic Evidence*. Oakland: University of California Press.

Marshall P (2020) The harm that judges do-misunderstanding computer evidence: Mr Castleton's Story 'an affront to the public conscience'. *Digital Evidence & Electronic Signature Law Review* 17*:* 25–49.

McCartney C and Shorter L (2020) Police retention and storage of evidence in England and Wales. *International Journal of Police Science & Management* 22(2): 123–136.

Moorhead R, Nokes K and Helm R (2021) Post office scandal project: issues arising in the conduct of the bates litigation. Available at: https://evidencebasedjustice.exeter.ac.uk/wp-content/uploads/2021/08/WP1-Conduct-of-the-Bates-Litigation-020821.pdf (accessed 3 October 2022).

Muir R and Walcott S (2021) *Unleashing the Value of Digital Forensics.* London: The Police Foundation. Available at: www.police-foundation.org.uk/publication/unleashing-the-value-of-digital-forensics/ (accessed 12 May 2022).

National Police Chiefs Council (NPCC) (2020) Digital forensic science strategy. Available at: www.npcc.police.uk/Digital%20Forensic%20Science%20Strategy%202020.pdf (accessed 1 February 2021).

Page H, Horsman G, Sarna A, et al. (2019) A review of quality procedures in the UK forensic sciences: What can the field of digital forensics learn? *Science & Justice* 59(1): 83–92.

Ramirez F (2022) The digital divide in the US criminal justice system. *New Media & Society* 24(2): 514–529.

Richardson V, Hanway P, Baxter R, et al. (2022) Using appeal judgement transcripts to assess changes in the presence of digital evidence in police investigations. Home Office. Available at: www.gov.uk/government/publications/digital-evidence-in-appeal-judgement-transcripts/using-appeal-judgement-transcripts-to-assess-changes-in-the-presence-of-digital-evidence-in-police-investigations (accessed 20 September 2022).

Stoykova R (2021) Digital evidence: Unaddressed threats to fairness and the presumption of innocence. *Computer Law & Security Review* 42*:* 105575.

Stoykova R (2022) Standards for Digital Evidence: an inquiry into the opportunities for fair trial safeguards through digital forensics standards in criminal investigations. [Thesis fully internal (DIV), University of Groningen]. University of Groningen. https://doi.org/10.33612/diss.222646186 (accessed 5 April 2023).

Tully G (2020) *Forensic Science Regulator Annual Report 2018-2019*. London: Home Office. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/877607/20200225_FSR_Annual_Report_2019_Final.pdf (accessed 21 November 2021).

Warren RB and Salehi N (2022) Trial by file formats: Exploring public defenders' challenges working with novel surveillance data. *Proceedings of the ACM on Human-Computer Interaction* 6(CSCW1): 1–26.

Welsh L and Clarke A (2021) United by cuts: Exploring the symmetry between how lawyers and expert witnesses experience funding cuts. *Amicus Curiae* 2(3): 455.

Wilson-Kovacs D, Rappert B and Redfern L (2022) Dirty work? Policing online indecency in digital forensics. *The British Journal of Criminology* 62(1): 106–123.

Wilson-Kovacs D and Wilcox J (2022) Managing policing demand for digital forensics through risk assessment and prioritization in England and Wales. *Policing: A Journal of Policy and Practice*. https://academic.oup.com/policing/advance-article/doi/10.1093/police/paac106/6917132 (accessed 3 January 2023).