This paper has been updated and will be published in The Criminal Law Review. Please note it may differ from the final published version.

The Evidential Value of Electronic Communications Data in Rape and Sexual Offence Cases

Philip N.S. Rumney* and Duncan McPhee**

Key words: electronic evidence, rape, sexual offences, police, prosecutors

There is much controversy concerning police requests for access to electronic devices and online data from rape complainants. Critics have expressed concern that allowing such access enables the police and potentially, prosecutors and defence lawyers, to examine large amounts of material, including photographs, texts and email, that maybe irrelevant to the investigative and prosecutorial process.[1] It has been argued that these requests, or "demands" and "digital strip searches",[2] as they are often described, are increasing;[3] that they adversely impact on the wellbeing of complainants; infringe a complainant's right to privacy[4] and deter engagement with the criminal justice process.[5] In addition, successive Victims' Commissioners for England & Wales have criticised the extent of data access requests and their impact on complainants.[6] In February 2019, the National Police Chiefs'

* Professor of Criminal Justice, De Montfort University School of Law. E-mail: phil.rumney@dmu.ac.uk

** Senior Lecturer in Criminology, University of the West of England.

[1] See for example, O. Bowcott, "Rape cases 'could fail' if victims refuse to give police access to phones" *The Guardian* 29 April 2019 https://www.theguardian.com/society/2019/apr/29/new-police-disclosure-consent-forms-could-free-rape-suspects [Accessed 30 September 2010]; Barr and Topping, fn. 17 below.

2 Big Brother Watch, *Digital Strip Searches: The police's data investigations of victims* (2019), pp. 9, 1.

[3] A recent HM Crown Prosecution Service Inspectorate report (hereafter HMCPSI) found that most surveyed CPS lawyers (70.5%) and managers (78%) believed that electronic data requests had increased since January 2018: HMCPSI, *2019 Rape Inspection: A thematic review of rape cases by HM Crown Prosecution Service Inspectorate* (2019), Table 1. This, of course, is impressionistic and more robust data is needed. At the time of writing, the Victims' Commissioner for London and the Mayor's Office for Policing and Crime are engaged in a study of police electronic data requests, their impact and criminal justice outcomes, which will hopefully provide better quality data: O. Bowcott and C. Barr, "Impact on rape victims of police phone seizures to be reviewed" *The Guardian* 16 February 2020 https://www.theguardian.com/society/2020/feb/16/impact-on-victims-of-police-phone-seizures-to-be-reviewed [Accessed 30 September 2020].

[4] Information Commissioner's Office, *Mobile Phone Data Extraction by police forces in England and Wales* (2020).

5 Bowcott, fn. 1 above.

[6] Victims' Commissioner for England & Wales, *Annual Report of the Victims' Commissioner 2018 to 2019* (2019), p. 36 https://victimscommissioner.org.uk/annual-reports/annual-report-of-the-victims-commissioner-2018-to-2019/ [Accessed 30 September 2020] (Baroness Newlove of Warrington: "Victims of sexual violence are routinely having their personal lives disproportionately investigated and disclosed in criminal trials"). M.

Council (hereafter NPCC) introduced a digital evidence consent form for victims and witnesses.[7] The lawful basis of the NPCC's documentation, along with its implications for complainant privacy and psychological welfare has been the subject of criticism by campaign groups,[8] the Court of Appeal in *Bater-James*[9] and a report issued by the Information Commissioner's Office (hereafter ICO),[10] As a result, the NPCC announced it would withdraw and replace the form,[11] which it did in September 2020.[12]

The purpose of this article is to examine new evidence derived from a study of police case file data and address issues that have been largely ignored in the current controversy. Specifically, this paper will identify the types of evidence produced by electronic data requests from devices used by rape complainants and those seized from suspects, along with the ways in which the data was of assistance to the police, Crown Prosecution Service and defence. In addition, the article will address the issue of data access requests in cases involving historic allegations of rape and the role electronic data play in assisting the police in addressing the intimidation of complainants by suspects and third parties.

1. The existing research evidence

The purpose of this section is to examine existing research findings derived from official reviews and inspectorate reports, academic analysis, and specialist sector research to identify areas for concern in current criminal justice practice.

Oppenheim, "Rape cases dropped over 'unlawful' police demands for access to victims' phones" *The Independent* 23 July 2019 https://www.independent.co.uk/news/uk/home-news/rape-cases-police-data-big-brother-watch-a9017166.html [Accessed 30 September 2020] (Dame Vera Baird: "Unless they sign the entire contents of their mobile phone over to police search, rape complainants risk no further action on their case. These are likely to be traumatised people who have gone to the police for help").

[7] The document is entitled: "Digital device extraction – information for complainants and witnesses". The full text is embedded in the following source: Bowcott, fn.1 above.

[8] Bowcott, fn.1, above.

[9] *Bater-James and Mohammed* v *R* [2020] EWCA Crim 790. Hereafter *Bater-James*.

[10] ICO, fn. 4, above.

[11] National Police Chiefs' Council, "Police and prosecutors to replace consent form for digital evidence" 16 July 2020 https://news.npcc.police.uk/releases/police-and-prosecutors-to-replace-consent-form-for-digital-evidence [Accessed 30 September 2020]. In a letter to Chief Constables, by Assistant Chief Constable Tim De Meyer, the NPCC lead on Disclosure the interim guidance and consent documents "will be circulated by the NPCC and forces should immediately adopt them in order to comply with *Bater-James*".

[12] National Police Chiefs' Council, "Police replace processing notice used to obtain agreement from victims and witnesses to search for relevant material on digital devices" 2 September 2020 https://news.npcc.police.uk/releases/police-replace-processing-notice-used-to-obtain-agreement-from-victims-and-witnesses-to-search-for-relevant-material-on-digital-devices [Accessed 30 September 2020]. NPCC notes: "The interim forms will implement the principles set out in the *Bater-James* judgment, pending a permanent replacement being produced following further engagement with stakeholders".

England and Wales

The issue of harm caused to complainants by police electronic data requests has been commonly referenced but the subject of only limited research. A survey in England and Wales conducted by *The Guardian* newspaper and Rape Crisis England & Wales,[13] and a report by Big Brother Watch have highlighted the distress, aggravation of trauma and disengagement from the investigative process that may be caused by data access requests.[14] Following on from these concerns, a recent report by the ICO observed: "It is … critically important that individuals who have been a victim of or witness to crime do not suffer further distress due to unnecessary intrusion into areas of their life they have a reasonable expectation would be kept private".[15] The Big Brother Watch report[16] and a recent report by the HM Crown Prosecution Service Inspectorate (hereafter HMCPSI)[17] expressed concern about the time taken to analyse large amounts of electronic data in sexual offence cases. Big Brother Watch also notes variations between force areas in the time taken for electronic devices to be examined[18] and the use of extraction software that gathers excessive amounts of personal data, despite the availability of alternative software that can target sought after material.[19] The HMCPSI report found another cause of excessive data downloads that impact complainants and suspects. That is, requests by prosecutors: "Some prosecutors are still asking for a full download of a complainant's or suspect's phone. We think this may be because of a lack of awareness of the types of download that are available, and what they can provide".[20] Subsequently, the court in *Bater-James* suggested a more appropriate approach - where it is necessary to look at a complainant's phone a "critical question" to consider is whether it is possible to view a limited amount of data such as a string of messages.[21]

Evidence derived from Freedom of Information Act 2000 (hereafter FOI) requests has been produced by *The Guardian* newspaper suggesting the existence of differing data requesting practices between police forces, amounting to a "postcode lottery" in which personal data

[13] For discussion of these and other findings, see: fnn. 74-75 below and accompanying text.

[14] Big Brother Watch, fn. 2 above, pp. 47-50.

[15] ICO, fn. 4 above, p. 16.

[16] Big Brother Watch, fn. 2 above

[17] HMCPSI, fn. 3 above, para. 4.29.

[18] Big Brother Watch, fn. 2 above, p. 18. (in a survey of 12 force areas, the shortest time period was 4 weeks and by contrast, the longest waiting time was up to 9 months).

[19] Big Brother Watch, fn. 2 above, pp. 12-13, 17-19, For this issue more generally, see: Privacy International, *Digital stop and search: how the UK police can secretly download everything from your mobile phone* (2018).

[20] HMCPSI, fn. 3 above, para. 5.52.

[21] *Bater-James*, fn. 9 above, para. 88.

was requested in two force areas and none in a third.[22] The report only makes explicit reference to three force areas, with mention of electronic data in only one and there is no indication of how many FOI requests were made. While the issue of varied practice between force areas is undoubtedly troubling, the lack of detail as to what was found through the FOI requests makes it difficult to judge the specific issue of variability or whether the reported practices were widespread. Similar problems can be attributed to another widely disseminated newspaper report on results from a survey of frontline specialist support workers. *The Guardian* and Rape Crisis England & Wales found that "[a]s many as eight in 10 rape complainants in some police force areas are being asked to disclose personal data from their phones during investigations …".[23] *The Guardian* notes: "[t]he figures are a snapshot of current cases of rape complainants across 12 Rape Crisis centres in England & Wales in the last week of August [2019] and 20 ISVAs [Independent Sexual Violence Advocates] at various centres earlier in the year".[24] Given the lack of detail it is difficult to assess the methodology and applicability of the eight in 10 figure. First, it is unclear whether the collected data were gathered from written records, relied on the memory of frontline workers or how many frontline workers were consulted. Second, it is unclear how many rape complainants the frontline staff dealt with. Likewise, the timeframe of cases included in the survey is unknown. Third, it is unclear how many force areas were covered in the survey and how many forces had a similar or lower rate of complainant data access requests. The story's reference to 12 Rape Crisis centres and an additional 20 ISVAs would suggest, some, perhaps most force areas were excluded. While a crude comparison, because of differences in methodology, the eight in 10 figure can be compared to data produced by the 2019 London Rape Review which found reference to social media in 13% of reviewed cases and complainant or suspect technology in 17% of cases.[25]

---

[22] C. Barr and A. Topping, "Police demands for potential rape victims' data spark privacy fears" *The Guardian* 25 September 2018 https://www.theguardian.com/society/2018/sep/25/revealed-uk-police-demanding-access-data-potential-rape-victims [Accessed 30 September 2020]. Big Brother Watch has also used FOI requests to examine *inter alia* what occurs if a rape complainant refuses to allow police access to his or her phone. The group found that in "100% of cases where victims refused to hand in phones were dropped": "Rape Cases Dropped Over Digital Strip Search Refusals" 18 June 2020 https://bigbrotherwatch.org.uk/2020/06/rape-cases-dropped-over-digital-strip-search-refusals/ [Accessed 19 September 2020].

[23] C. Barr, "People who report rape face 'routine' demands for their mobile data" *The Guardian* 21 September 2019 https://www.theguardian.com/society/2019/sep/21/people-report-rape-routine-demands-mobile-data?CMP=Share_iOSApp_Other [Accessed 3 May 2020]. In addition to this figure, the survey found: "The majority [of frontline staff] also noted that the requests were happening in some rape cases involving a stranger (61%)". On its face, this finding is troubling assuming that "stranger" only involves cases where the complainant and suspect are unknown to each other or where there is no post-rape electronic contact between the suspect and complainant. However, "stranger" is not defined in the report, nor is it clear whether any data requests related to matters to help identify the suspect (e.g. photos).

[24] Barr, fn. 23 above.

[25] Mayor of London Office for Policing and Crime, *The London Rape Review: A review of cases from 2016* (2019), p. 33.

North America

It appears that the police's use of electronic data requests in sexual offence cases in England and Wales has received significantly more attention than such requests have in any other jurisdiction. This is surprising given the widespread use of mobile phones and other technology and because the issues of concern in England and Wales, including complainant privacy, are likely to be similar across many jurisdictions.[26] The evidence that does exist originates from North America and includes a case study featuring the use of electronic data in a North American intimate partner abuse case,[27] and the use of phone text evidence in two North American sexual assault trials.[28] Recent research, based on interviews with Canadian police officers, found that they believed electronic evidence to be useful in case building,[29] but also acknowledged the emotional distress caused to complainants by electronic data requests.[30] In addition, they observed that accessing and analysing digital evidence could slow the investigative process.[31]

The Canadian research suggests similar problems and dilemmas to those found in England and Wales. From this review, however, it is evident that there exists relatively little robust empirical data to help guide analysis and policy development. Small scale studies may provide important clues to wider trends and qualitative data can be crucial in improving our knowledge of the impact of police and prosecutorial practice, but it leaves many gaps in our current understanding.

2. Accessing electronic data and complainant consent

In order to address the growing concerns over electronic data requests discussed earlier,[32] the NPCC has recently issued revised interim documentation in the form of a "Digital

[26] It is feasible that legal privacy protections have impacted police practice in some jurisdictions, although without detailed legal and empirical analysis it is impossible to know for certain.

[27] F.A. Ramirez and J. Lane, "Communication Privacy Management and Digital Evidence in an Intimate Partner Violence Case" (2019) 13 *International Journal of Communication* 5140.

[28] H.R. Hlavka and S. Mulla, "'That's How She Talks': Animating Text Message Evidence in the Sexual Assault Trial" (2018) 52 *Law & Society Review* 401.

[29] A. Dodge *et al*, "'This isn't your father's police force': Digital evidence in sexual assault investigations" (2019) 52 *Australian & New Zealand Journal of Criminology* 499, p. 509 (noting *inter alia* that "digital evidence … can act as 'digital breadcrumbs' … that lead to the offender. In some cases, it challenges the 'he-said she-said' … nature of sexual assault cases and provides evidence that lessens the well-documented burden of testimony for sexual assault victims" [internal citations omitted]).

[30] Dodge *et al*, fn. 29, above.

[31] Dodge *et al*, fn. 29 above, pp. 505-508, 510-12. Officers also noted the need for training and improved technological and human resources in order to address the growth in the use of electronic evidence (pp. 505-508)

[32] For discussion, see: fnn. 8-10 above and accompanying text.

Processing authorisation form" which includes guidance for police officers[33] and a second document, entitled "Victim/Witness FAQ". These are now used in all force areas.[34] In the officer guidance document explicit reference is made to the Court of Appeal decision in *Bater-James* and is drafted in light of the decision.[35] The guidance reminds officers that an electronic device "should not be sought on the basis of mere conjecture or speculation". Instead, electronic data must be part of a reasonable line of enquiry: "You must have a properly identifiable basis for forming your belief that specific material is required from the device".[36] Indeed, officers have to explain in writing the basis for this belief[37] and why it is "proportionate and strictly necessary to extract material from the device". Further, officers must explain why alternatives to accessing the complainant's device have been rejected.[38] This latter point is an important matter of investigative focus. The 2015 *Joint CPS and Police action plan on rape* emphasises the importance of an offender-centric approach to rape investigation, with a "focus on the actions of the offender, rather than those of the victim".[39] The adoption of such an approach should see an initial focus on the offender's device(s) as suggested in *Bater-James*: "the investigator will need to consider whether, depending on the apparent live issues, it may be possible to obtain all the relevant communications from the *suspect's* own mobile telephone or other devices without the need to inspect or download digital items held by the complainant"[40] (emphasis in original). The NPCC officer guidance appears to take a different approach. It sets out two questions for officers to consider: "Have I already obtained the same material from the suspect's device? If so, is this sufficient to mean I do not need to examine the [complainant's] device?".[41] The difference between the approach in *Bater-James* and in the NPCC guidance is one of priorities. The questions posed in the guidance appear in a section that presupposes the complainant has already agreed to a data access request and offers guidance on what and how electronic data should be reviewed.[42] By contrast, the information for victims and witnesses states on the first page: "We will … consider whether

[33] NPCC, "Digital Processing Authorisation Form (DPNa)"/"Guidance for Officers Completing the Form – FAQs" (2020).

[34] NPCC, "Victim/Witness FAQ - Digital Processing Notice b (DPNb)" (2020).

[35] NPCC, fn. 33 above, p. 5.

[36] NPCC, fn. 33 above, p. 5.

[37] NPCC, fn. 33 above, p. 1.

[38] NPCC, fn. 33 above, p. 2

[39] *Joint CPS and Police Action Plan on Rape* (2015), p. 3. https://www.cps.gov.uk/sites/default/files/documents/publications/rape_action_plan_april_2015.pdf [Accessed 25 September 2020].

[40] *Bater-James*, fn.9 above, para. 78.

[41] NPCC, fn. 33 above, p. 5.

[42] NPCC, fn. 33 above, p. 5.

there are other ways to obtain the material we need before asking you to hand over your device".[43] The possibility of gaining all necessary evidence from the suspect's device, thereby *avoiding* a potentially distressing discussion with the complainant concerning data access is not referenced in the officer guidance. On the grounds of minimising complainant distress and following an offender-centric policing approach, a clear statement in the officer guidance that an examination of the suspect's device(s) is to be prioritised better reflects the decision in *Barter-James*, even if data is sought from the complainant's device(s) at a later time.

The officer guidance makes clear that without the complainant's agreement, electronic data cannot be accessed. Where a device is examined, the guidance stipulates that only relevant material should be sought using "the least intrusive method where appropriate".[44] Officers are expected to explain to complainants the reasons for seeking the electronic data, the nature of the data sought, the length of time the police will need to keep the device and the potential implications of a complainant refusing access to an electronic device.[45] There is no guidance given to officers on what constitutes "agreement", nor a warning that the capacity of complainants to validly consent to handing over their device(s) and subsequent data downloading might be affected by the trauma of sexual victimisation. The ICO report states that due to the trauma caused by rape, it is "important that police consider the cognitive ability of post-trauma victims to be able to rely on Consent for processing personal data".[46] Importantly, the "Victim/Witness FAQ" document makes clear that a complainant does not have to agree to a data access request. In such circumstances, the FAQ states: "If you decide not to give us the device, we will ask you to provide reasons and work with you to address your concerns. Our aim is to reassure you of the good reasons for extracting material and that the extracted material will be kept securely".[47] One potential reason for a complainant's refusal to allow access to a device is the time a device may be kept by the police. One means of addressing such concerns is referenced in the officer guidance and "Victim/Witness FAQ". The documents acknowledges that it might be possible to record electronic data without depriving the complainant of their phone or device.[48] For example, by the use of screenshots.[49] The officer guidance is undoubtedly helpful in focusing the minds of officers, requiring specific reasons for decisions and for advice intended to reduce complainant distress. However, given the interim nature of the guidance and

[43] NPCC, fn. 34 above, p. 1.

[44] NPCC, fn. 33 above, p. 5-6.

[45] NPCC, fn. 33 above, pp. 7-8.

[46] ICO, fn. 4, above, p. 36.

[47] NPCC, fn. 34 above, p. 1.

[48] NPCC, fn. 33 above, pp. 5-6; NPCC, fn. 34 above, p. 2. ("If possible, we will obtain the material we need without taking your device from you").

[49] NPCC, fn. 33 above, pp. 5-6.

"Victim/Witness FAQ" there are several areas discussed here that require further attention.[50]

3. Methodology

This paper provides new data based on a study of 441 police case files involving rape investigations featuring male and female complainants who were 14 years' and older at the time of reporting. The data were gathered from two different policing areas and covered all rape investigations over a two-year period. For this article, the collected file data were searched for reference to communications evidence, specific words such as 'text' and 'email' and devices such as phones, laptops, and specific social media platforms. This produced 61 cases in which there was a complainant data access request or seizure of a suspect's device(s). Requests and seizures were made in relation to phones, laptops, and computers, along with several social media platforms. In 70.4% of cases (43 out of 61) the police sought data from complainant and/or suspect phones. Given these data were gathered from police case files, with a specific focus on the investigative stage of the criminal justice process, there is no data that would inform a useful discussion of the disclosure of unused prosecution material to the defence[51] or disclosure of evidence to the suspect or his/her lawyer under the Police and Criminal Evidence Act 1984 Code of Practice.[52]

The 441 cases include those where there was no prospect of accessing electronic evidence, such as when a suspect could not be identified or where a complainant reported to the police, but did not want a formal police investigation. This article includes reference to charging and convictions in rape and sexual offence cases. To avoid double counting, where a defendant was convicted of multiple offences the most serious offence in terms of maximum sentence is counted. In only one case was a defendant convicted of a non-sexual offence, but is included in this study because he was also convicted of a sexual offence. The police investigations from which these data originates took place prior to the Liam Allan case[53] and Crown Prosecution Service investigation that uncovered 47 cases in which there

[50] NPCC, fn. 12, above (noting the need for the "permanent replacement" document to "fully" address the recommendations contained in the recent ICO report, along with input from other stakeholders).

[51] As regulated by the Criminal Procedure and Investigations Act 1996 (as amended). For further discussion, see: Smith, fn. 53 below.

[52] See: Home Office, Code C, *Code of Practice for the detention, treatment and questioning of persons by Police Officers* (Revised, 2019), para. 11.1A.

[53] For discussion, see: T. Smith, "The 'near miss' of Liam Allan: Critical Problems in Police Disclosure, Investigation Culture, and the Resourcing of Criminal Justice" [2018] Crim. L.R. 711, 715; Crown Prosecution Service, *Rape and serious sexual offence prosecutions - Assessment of disclosure of unused material ahead of trial* (2018).

were problems with disclosure of unused material to the defence.[54] Given the potential impact of these developments on the number of data access requests and evidence that such requests are increasing,[55] the authors do not claim the number of data access requests or seizures in this article reflect current practice.[56] Thus, the focus of this article is on the *types of evidence* produced by data access requests and the *assistance* it gives to the police, prosecutors and defence.

4. The use and type of electronic data

Of the 61 cases in the total sample, electronic data were derived from the complainant's device(s)[57] (24 cases), suspect device(s) (12); complainant and suspect device(s) (6), and no information was available to identify the owner/user of device(s) (16). There were also two data access requests that were refused[58] and another case in which a requested phone was lost by the complainant (3). The disparity between the number of suspect and complainant devices that were accessed is partly explained by four cases in which complainants had been sent intimidating phone or online messages. In those cases, gaining access to the complainant's phone or social media platform was important in order to examine the messages and identify the sender. Ultimately, it is not possible to fully explain the disparity, in part due to the number of "no information" cases in the sample. This leaves open the possibility that other, unidentified factors, were at play, including a point highlighted by the court in *Bater-James* - whether officers gave sufficient attention to the possibility that all relevant electronic data could be gathered from the suspect's phone.[59]

More recent data suggest similar request and seizure rates between complainants and suspects. In a recent HMCPSI inspection report, it was found that of "80 police admin finalised cases" 58 (72.5%) involved devices containing potentially relevant electronic data. Appropriate requests were made to access complainant devices in 89.7% of these cases and suspect devices were appropriately seized in 86.9% of cases.[60] Given concerns about the

[54] Crown Prosecution Service, *Rape and serious sexual offence prosecutions - Assessment of disclosure of unused material ahead of trial* (2018), p.4.

[55] HMCPSI, fn. 3 above.

[56] In this sample, the number of device access requests and seizures appear quite low (61/441). It cannot be assumed that this reflects post-Allan/CPS review practice.

[57] Reference to devices includes complainant and suspect social media platforms and email.

[58] Recent FOI data released by Big Brother Watch found that "at least 1 in 5 victims refused digital strip searches": "Rape Cases Dropped Over Digital Strip Search Refusals" 18 June 2020 {Accessed 30 September 2020] https://bigbrotherwatch.org.uk/2020/06/rape-cases-dropped-over-digital-strip-search-refusals/

[59] *Bater-James*, fn. 9 above, para. 78.

[60] HMCPSI, fn. 3 above, para. 5.51. Research by the Mayor of London Office for Policing and Crime, relying on cases from 2016, also found similar numbers of access requests and seizures (complainant devices: 11%; suspect devices: 13%): fn. 25 above, p. 37.

impact of access requests on the wellbeing of complainants and the limited existing evidence, the relative access request and seizure rate is undoubtedly a matter that requires further investigation.

In Figure 1, the data are divided in order to understand more fully the differing types of evidence produced from data access requests and seizures and the assistance it gave to the police, CPS and defence. It cannot be assumed that the existence of electronic communications evidence was the main reason for a case outcome or decision, but the nature of the evidence suggests that it was a factor of significance in some cases. However, the role of other factors cannot be discounted. For example, within the 61 cases examined here, there was one case in which no relevant evidence was found on the complainant's or suspect's electronic devices, but the suspect was still charged with rape. This is a reminder that electronic evidence is part of a larger case building process.

All the cancelled cases involved police decisions in which it was decided that in line with the Home Office Counting Rules (hereafter HOCR), there existed "additional verifiable information" that determined no crime occurred.[61] In such cases, an initially recorded offence is removed from the constabulary's count of recorded offences.[62] Electronic communications data was not the only evidence considered by officers, although in some cases it provided compelling evidence that no crime occurred. For example, in one HOCR-compliant case consensual sex between the suspect and complainant was recorded and proved the specifics of the complainant's allegation to be untrue. In the two HOCR non-compliant cases, phone data contradicted statements made by the complainant but this, and other evidence, was determined by the research team to be insufficient to determine that no crime occurred.

[61] Home Office, *Crime Recording General Rules* (2020), Section C2.

[62] Home Office, *Crime Recording General Rules* (2020), Section C.

Figure 1

References to data derived from electronic devices in case files (n=61)

Category	Number of cases and percentage
1. Data access request refused, or phone lost	3 (4.9%)
2. No relevant evidence found	7 (11.4%)
3. Relevant evidence in HOCR compliant cancelled case	4 (6.5%)
4. Relevant evidence in HOCR non-compliant cancelled case	2 (3.2%)
5. Evidence assisting police and prosecution	22 (36.0%)
6. Evidence assisting defence[63]	19 (31.1%)
7. Evidence of intimidation directed at the complainant	4 (6.5%)

In the 22 cases where evidence assisted the police and prosecutors, 13 (59.0%) led to the suspect being charged with a sexual offence and 10 resulted in conviction for any sexual offence (45.4%) and, of these, six cases resulted in a rape conviction (27.2%).[64] In all these conviction cases, electronic evidence from a complainant and/or suspect's device or social media account played a role in the suspect being identified and arrested. It is also likely to have played a role in the decision to charge.[65] For example, in one case evidence from a victim's phone featured an admission by the offender and provided corroborative evidence that she was a victim of child sexual abuse. In another case, an offender apologised via text for sexually abusing his victim and in a third, an offender's phone contained film of him raping his victim. In a fourth case, social media posts were the means by which a rapist was identified by his victim. This finding reflects the value of electronic evidence in the

[63] Given the nature of the police case file data, there was no information concerning the views of defence lawyers. Instead, the authors assessed the potential assistance of electronic data to the defence in light of rules that require disclosure of evidence that undermines the case for the prosecution or assists the defence: Crown Prosecution Service, "Disclosure – Guidelines on Communications Evidence" (2018) https://www.cps.gov.uk/legal-guidance/disclosure-guidelines-communications-evidence [Accessed 3 May 2020].

[64] In terms of the total sample of 61 cases, the respective rates are 21.3% (charged); 16.3% (convicted of any sexual offence) and 9.8% (convicted of rape). The 61 cases includes the three where devices could not be examined due to two complainants refusing data access requests and the one case in which a phone was lost.

[65] On the issue of charging decisions, see fn. 79 below.

successful prosecution of some sex offenders that can also be found in decisions of the Court of Appeal.[66]

Concern has been expressed about data access requests involving cases of historic sexual abuse where there is a large gap between reporting and the alleged offence(s) or where the alleged offence(s) occurred prior to the widespread use of mobile phones.[67] Indeed, the Director of Public Prosecution's *Guide to "reasonable lines of the enquiry" and communications evidence*, states that there is "no requirement" for an examination of an electronic device in cases featuring *inter alia*: "historic allegations where there is considered to be no prospect that the complainant's phone will retain any material relevant to the period in which the conduct is said to have occurred and/or the complainant through age or other circumstances did not have access to a phone at that time".[68] This, we argue is entirely correct. However, there might be rare cases where electronic communications evidence is of importance even in the circumstances set out by the DPP guide. For example, where there is ongoing contact between a suspect and complainant. In such circumstances there might be relevant evidence on a device acquired many years after a sexual offence has been committed, such as where the suspect apologises for his or her offending behaviour.[69] However, confessions in these circumstances are probably very rare. Confessions are more likely where police have found a device containing "text messages between a minor and an adult" which police may then use to "elicit a confession and reduce the stress on witness testimony".[70]

In the current sample, seven cases involved allegations of a historic nature.[71] In terms of complainant devices, these requests did yield useful evidence in two categories of case: a complainant intimidation case (1) and cases in which electronic data contradicted clams made by the complainant and so assisted the defence (3). Suspect devices in historic cases were also useful to officers: where phone data proved the suspect lied to officers (1) and

[66] See for example, *R* v *Hart* [2019] EWCA Crim 270 (offender contacting his victim via phone calls and texts led to her reporting sexual abuse to the police at which point the offender admitted his guilt). *R* v *Lewis* [2019] EWCA Crim 710; *R* v *Merchant* [2018] EWCA Crim 2606; *R* v *JWW* [2019] EWCA Crim 1273 (electronic communications evidence providing evidence that assisted the prosecution). *R* v *Daviesi* [2018] EWCA Crim 2566 (electronic communications evidence providing evidence that assisted the prosecution in a case of historic sexual offending).

[67] A. Topping, "Data gathering 'may deny rape victims access to justice'" *The Guardian* 17 October 2018 https://www.theguardian.com/society/2018/oct/17/data-gathering-may-deny-victims-access-to-justice [Accessed 30 September 2020].

[68] 24 July 2018, para. 13. https://www.cps.gov.uk/legal-guidance/disclosure-guide-reasonable-lines-enquiry-and-communications-evidence [accessed 30 September 2020].

[69] While not a historic case, see Section 4 above for an example of a case in which a suspect makes an unprompted apology to his victim.

[70] Dodge *et al*, fn. 29 above, p. 11.

[71] "Historic" in this context, is defined as a report that is made to the police a year or more after the offence(s) allegedly occurred.

where examination of phone data led to the discovery of additional sexual offences (2). In these historic cases, ongoing contact between the complainant and suspect, sometimes many years after the alleged offence(s) occurred, resulted in the discovery of electronic evidence of assistance to the police, prosecutors, and the defence.

In 19 cases, electronic evidence assisted the defence and was predominantly made up of texts or social media posts that contradicted or in some other way undermined statements made by the complainant. In five of these cases, complainants made provably false statements to the police or other witnesses. For example, during the investigation, one complainant lied to officers about two matters - one of which involved sending himself threatening text messages that he falsely claimed were from someone else. In another case, the complainant sent messages instructing friends to lie to police officers about matters of importance to the case. While this does not mean there was no rape in these two cases,[72] other evidence that contradicted the complainants' statements and the proven falsehoods were seen by officers to undermine their credibility. In addition to the electronic communications evidence in the 19 cases, there was witness and CCTV evidence that contradicted or otherwise undermined complainant statements and little or no corroborative evidence that pointed to the guilt of the suspects. None of the 19 cases proceeded to charge. Dodge argues that "[w]hile defendants must be given a fair trial and allowed to utilise relevant digital evidence, there is a renewed need to reject the use of evidence that relies on stereotypes about sexual violence and sexual violence victims".[73] This issue emerges in one of the 19 cases. An officer took issue with texts between the complainant and suspect in which she said they would continue to be friends. The officer viewed the exchange as undermining the complainant's credibility. Of course, such texts might be helpful to the defence, but the officer's interpretation of the exchange rests on an expectation of appropriate victim behaviour which does not take into account, for example, efforts to pacify an offender, encourage a confession or remain friendly until the victim decides what to do next.

One of the criticisms of police requests for data access has been the potential impact on complainants. A survey published by *The Guardian* found that "[a]lmost all (95%) [of Rape Crisis frontline staff] said the requests had a negative impact on complainants, with some noting it deterred people from coming forward".[74] Disclosure of personal information to the

[72] For discussion, see: C.L. Saunders, "The Truth, the half-truth, and nothing like the truth: Reconceptualizing false allegations of rape" (2012) 52 *British Journal of Criminology* 1152, p. 1160 (noting the existence of "false accounts", that she describes, thus: "a false account of rape does not equate to establishing—or suspecting—that no rape, in fact, occurred. Rather, this is an allegation of rape containing statements of fact that are inaccurate and, consequently, not true"). False accounts might involve deliberate falsehoods, but complainants might also make false claims in error or as a result of trauma, embarrassment or a fear that they will not be believed by criminal justice professionals.

[73] A. Dodge, "The digital witness: The role of digital evidence in criminal justice responses to sexual violence" (2017) *Feminist Theory* 1, p. 14.

[74] Barr, fn. 18 above.

police is undoubtedly troubling to complainants: it may cause embarrassment, fear, anxiety and exacerbate the trauma of rape.[75] Thus, data access requests and disclosure of personal information may manifest themselves in a complainant withdrawing an allegation. While it is possible that data access requests may have had this impact in some individual cases, the quantitative evidence in the sample featured here does not suggest a relationship between access requests and withdrawal. In crimed cases[76] featuring an electronic data access request from a complainant's device(s) or social media account, the withdrawal rate was 21.2% (7 of 33). This was lower than the withdrawal rate for crimed cases generally in the total case sample - 32.0% (121 of 377).

Further, withdrawal data require careful analysis because it cannot be assumed that withdrawal occurs for a single reason when it may have complex and multiple causes. While a relationship between data access requests and withdrawal is not suggested by the quantitative data, qualitative data may yield important insights. However, it is apparent that the potential impact of data access requests are not generally referenced in the qualitative data – with one exception. In one case, the complainant withdrew after the police were unable to provide a replacement phone of the exact model that was requested. It is unclear why this model was important, though the request may have been linked to its functionality. This reason is unique to the dataset and does not readily fall into the category of case in which withdrawal is said to result from distress caused by an access request.[77]

Of the remaining six withdrawal cases, three involved reports that were made by third parties and despite efforts to encourage engagement, the complainants in these cases made clear that they did not wish to support the respective investigations.[78] In the other three cases, reasons to withdraw included: a fear of the court process; a wish to "move on" and a complainant stating that she did not want to think about the rape anymore. Where electronic data was gathered by the police in the withdrawal cases, it pertained mainly to disclosure of the alleged rape to a third party, including disclosures made immediately following an alleged rape and evidence of intimidation directed at the complainant. In two of the six cases, officers were confident the suspects would be charged by the CPS, but

[75] See for example, A. Mohdin and C. Barr, "'I was devastated': the crime victims made to give up their phones" *The Guardian* 21 September 2019 https://www.theguardian.com/society/2019/sep/21/devastated-crime-victims-made-to-give-up-phones [Accessed 3 May 2020]. See also: Big Brother Watch, fn. 14 above and accompanying text.

[76] Those reports recorded as offences of rape in accordance with the Home Office Counting Rules, fn. 61 above, Section A.

[77] The complainant had previously expressed some doubts about supporting the investigation. It is possible that this also influenced the decision to withdraw.

[78] Indeed, it is evident from the literature that third party reporting can cause distress to complainants, not least because it represents a loss of control over the decision to disclose to the police: O. Brooks-Hay, "Doing the 'right thing'? Understanding why rape victim-survivors report to the police" (2019) 15 *Feminist Criminology* pp. 15-16* (*the page citation is to the institutional repository version of this paper) http://eprints.gla.ac.uk/190358/1/190358.pdf [Accessed 30 September 2020].

following communication from the complainants that they wished to withdraw, and after efforts to encourage engagement, officers chose not to pursue the charging option. In the first case, a reviewing officer was concerned about losing the trust of a vulnerable complainant and in the other, an officer noted: "[being] mindful of conducting a victim-oriented investigation, I have no choice but to file this in accordance with the victim's wishes".

In the case file sample, there were two cases in which a data access request was refused and another case in which the complainant lost her phone. In the cases involving refusal, it is not known what reasons the complainants gave, but officers continued to pursue other lines of enquiry.[79] A recent report by HMCPSI found several reasons for the refusal of data access requests, including: privacy concerns; "adverse media coverage", "misunderstandings about what would happen to the material" and disproportionate CPS data requests.[80] As already noted, data access requests may yield important evidence, but they may also adversely impact the welfare of complainants. Thus, the impact of data access requests and the amount of data sought need to be carefully considered by police officers and CPS lawyers. In addition, it is crucial that police officers pursue all reasonable lines of enquiry, as continued investigation may build trust with a complainant and produce compelling new evidence, rendering communications data much less important.

Finally, research has long recognised that domestic violence perpetrators use threats and manipulation in an effort to control their partners and this may continue after abuse has been disclosed to law enforcement or specialist support agencies.[81] The case file data suggest that controlling behaviour can also extend to the suspect's friends and family members. Of the four complainant intimidation cases in the sample, two involved a history of domestic violence. In the first, a relative of a suspect sent abusive texts and the suspect himself used Facebook to disseminate a threatening message. In the second case, a complainant expressed a wish to withdraw her allegation following online threats and harassment by friends of the suspect.[82] In the other two cases, friends or family of the

[79] Indeed, there is no need for electronic communications data to be accessed in every case. Whether seeking access to such data is a reasonable line of enquiry will depend on the facts of each individual case: *R* v *E* [2018] EWCA 2426 (Crim).

[80] HMCPSI, fn. 3 above, para. 7.16. On the specific issue of appropriate requests by CPS lawyers, the HMCPSI report produced data that suggest the need for improvement. In only 60.9% of "admin finalised and charged or [No Further Action cases], the lawyer properly identified where an action did or did not need to be raised for a complainant's phone or other digital devices, and set out a proportionate request where it did" (para. 5.22).

[81] For example, see: M.L. Haselschwerdt and J.L. Hardesty, "Managing secrecy and disclosure of domestic violence in affluent communities" (2017) 79 *Journal of Marriage and Family* 556.

[82] In both domestic violence cases the police intervened. In the first case the suspect and relative were warned about their conduct. In the second case, threats led to an individual being arrested. At the time this data were collected the suspect was still under investigation.

suspect used phone messages, Facebook and other platforms to threaten and intimidate complainants.

Conclusion

These findings offer insight into the types of electronic communications evidence found in the case files featured in this research. The data from this study also indicate that evidence derived from social media, phones and other electronic devices assisted the police, prosecution, and defence. In some instances, this evidence was an important part of the case against a suspect and contributed to identification, arrest and likely, the decision to charge.[83] While in others, communication evidence undermined the credibility of a complainant's allegation. In a small number of cases phone data were crucial in enabling the police to identify and act against suspects or their associates who sought to intimidate complainants. The utility of electronic communications evidence is a factor that has been neglected during the recent controversy concerning police access to phones and other digital devices. Clearly, the development of good policy and practice requires careful data collection, evaluation and consideration of a wide range of factors, including the usefulness of electronic communications evidence as it pertains to complainants *and* suspects.[84] Further, Dodge *et al* note that: "interpretations of digital evidence … are malleable despite their 'neutral' appearance"[85] Indeed, one case in the current study contained a troubling interpretation of texts between the complainant and suspect that appeared to be based on a police officer's particular expectation of complainant behaviour. While not unique to electronic evidence, there is undoubtedly a need for a detailed examination of how such data are interpreted by police officers, prosecutors and defence lawyers.[86] Finally, as with all police case file data studies, these findings are specific to the sample of case files used here and cannot be assumed to apply to other force areas.

[83] The authors did not have access to CPS case files, but it seems likely given its nature, that electronic evidence played an important part in some charging decisions.

[84] In the current sample, 11.4% of device examinations produced no useful data. It might be that useful data was deleted by a suspect or complainant, but it also raises a question about the basis for the belief that device access requests/seizures were a reasonable line of enquiry in the first place.

[85] Dodge *et al*, fn. 29 above, p. 509.

[86] Dodge *et al*, fn. 29 above, pp. 509-510 (noting the danger of electronic evidence being used inappropriately by the defence and complainant texts etc. being interpreted through the lens of myths and stereotypes). Clearly, there is also the danger of electronic evidence being interpreted in a manner that is unfair to suspects and defendants.