Elizabeth Denham
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

By email only: [redacted]

9h November 2018

Dear Elizabeth Denham,

Complaint: The collection, analysis and disclosure of complainants of sexual offences' personal information and the use of 'consent' statements

We are writing to you to raise serious concerns about the access, collection, analysis and disclosure of complainants of sexual offences' personal information and the use of potentially coercive and overly-broad 'consent' statements by UK police forces and the Crown Prosecution Service (CPS). We have discussed our concerns with the Centre for Women's Justice and they support these submissions, although they will be be making their own additional submissions on this issue in due course.

Police, often under pressure from the CPS, are effectively investigating complainants – victims – of sexual offences' personal lives in the course of 'evidence gathering' as part of their investigations into sexual offences. Complainants' personal information may be subsequently disclosed as part of criminal investigations and trials. This process also involves the use of blanket 'consent' statements. We believe that the police and CPS' current policy, guidance and practice in relation to the collection, analysis and disclosure of complainants' information could break data protection laws and risk breaching the fundamental right to privacy protected by the European Convention of Human Rights.[1]

Digital evidence extraction

We are aware that you are conducting an investigation into mobile phone extractions, but as the issue of access, collection and extraction of digital information is a core part of current police and CPS practices considered in this complaint, we are addressing the issue holistically.[2]

Privacy International's investigation and report into police access to digital evidence found that different forces referred to different legal bases for their access to digital evidence, there was no

1 Article 8, European Convention of Human Rights.
2http://www.rasasc.org.uk/independent-sexual-violence-advocate-service/criminal-justice-system/

national guidance on police access to digital evidence, and police forces had differing local guidance or none at all.[3] One police force indicated that extraction of an individual's device was often carried out without the owner's knowledge.[4]

Complainants' digital evidence: access and collection

When a complainant reports a crime to the police, and indicates that there is relevant digital evidence on a device, such as a mobile phone, computer or tablet – any and all such relevant devices are typically taken from the complainant.

Since the General Data Protection Regulation (GDPR), some police forces are using 'Digital Processing Notices' to seek complainants' consent to the access and extraction of their digital devices, with differences between forces as to the content of these notices. However, we contend that it is inappropriate to request blanket consent, and that such blanket consent cannot be considered to be "freely given" as required by Article 7 and Recital 32 GDPR, under the Data Protection Act 2018. Complainants are informed that "limiting the information police download could have an adverse bearing" on their cases.[5]

Once the complainant's device or devices are taken by the police for forensic examination, they are held by police and will not be returned until the case is closed. Police may even require complainants' replacement phones which have been used whilst awaiting trial to be seized for further disclosure.[6]

Disproportionate collection

Complainants' devices may be either examined by police, or sent to an outsourced forensic facility. A complete copy of all the information on the device is made. This typically includes all texts, emails, pictures, videos, as well as any previously deleted data. Police can also request logins and passwords to complainants' social media accounts and personal 'cloud' storage services.

Digital devices will not only contain personal information about the complainant, but they will also contain information about their friends and family, including potentially sensitive communications, images, and other information. There also appears to be no restrictions or consistency in investigations as to the time frame of relevant material that may be accessed.

This disproportionate data collection can be especially intimidating in the context of the authorities collecting it. Information given to complainants threatens them that "if information is identified suggesting the commission of a separate criminal offence other than the offences under

---

3Privacy International, 'Digital Stop and Search', March 2018 (https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf)
4Derbyshire Police. In Privacy International, 'Digital Stop and Search', March 2018 (https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf)
5'Digital Processing notice' (Appendix 2)
6http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/justice-committee/disclosure-of-evidence-in-criminal-cases/written/80748.html

investigation…the relevant data will be retained and investigated… (…) This data may be shared with other parties including government agencies, defendants, legal representatives, as well as to a court in criminal proceedings".[7]

The Metropolitan Police has explained that the technology it currently uses – self-service kiosks – forces the download of all of a single type of information, even if only one element of that type of information is sought.[8] For example, this means that if police only need a single photo from a complainant's phone, the technology they currently have downloads all of the complainant's photos.[9] Furthermore, some digital forensics experts have also made the case that for forensic integrity of a single file to be maintained, using the police's current technology, an entire 'forensic copy' or 'image' of all the information on a digital device must be made at the beginning of an investigation.[10] Arguably, neither the police's digital forensics software nor their corresponding policies are fit for practice. The result is that complainants' data rights risk erosion and many report feeling that their private life is exposed. Arguably, such an indiscriminate download and investigation of data contradicts data protection laws as it falls outside of any rational notion of consent and constitutes disproportionate data processing. We believe this practice interferes with complainants' Article 8 right to a private life.

Excessive and disproportionate investigations of complainants

Police are required to explore all reasonable lines of inquiry in their analysis of digital information – and potentially, digital evidence – on complainants' devices. However, in practice, police can access, extract and analyse all of the information on a complainant's mobile phone or other device without practical restrictions, safeguards or oversight. Evidence indicates that police are in fact being pressured to conduct disproportionate searches by the CPS.

The Association of Police and Crime Commissioners (APCC) has called for an inquiry to examine the issue of complainants' information collection and subsequent disclosure issues. The APCC has stated that "evidence on the ground suggests that even when officers are confident that they have pursued all reasonable lines of inquiry, they are often being told by CPS to pursue all other available sources."[11]

The CPS often requires the police to gather information about a complainant of sexual violence from essential and sensitive public service providers. Police can and have requested information about complainants from healthcare providers, including complainants' mental health records, information from social services, educational establishments, counsellors and family court proceedings.[12] Unless

---

7 'Digital Device Downloads – information for complainants and witnesses' (Appendix 3)
8 https://www.documentcloud.org/documents/4348952-MET-Redacted-Self-Service-Equipment-Kiosk-Local.html in Privacy International, 'Digital Stop and Search', March 2018 (https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf)
9 https://www.telegraph.co.uk/news/2018/03/31/police-rolling-technology-allows-raid-victims-phones-without/
10 http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/justice-committee/disclosure-of-evidence-in-criminal-cases/written/80580.pdf
11 APCC calls for inquiry to look at all sides of disclosure – APCC, 14 February 2018: http://www.apccs.police.uk/latest_news/apcc-calls-inquiry-look-sides-disclosure/

this is done, it is reported that the CPS will not consider a charge.[13] It has also been reported that the CPS consistently rejects case files that do not have such third party material.[14]

Whilst police are questioning the need for so much information,[15] there appears to be no effective restriction on the CPS continuing to make disproportionate requests for information. There is a clear need for effective safeguards against such overly intrusive, overly-broad and irrelevant requests for complainants' personal information and records.

AI analysis

Recent reports that police and the CPS are trialling the use of artificial intelligence (AI) to trawl through digital evidence, including that of complainants of sexual offences, are extremely concerning.[16] The Metropolitan Police has confirmed[17] that it has been exploring Cellebrite's 'Analytics Enterprise' artificial intelligence tool, which can supposedly "detect and match objects within images and video such as weapons, money, nudity and more"; use "automatic facial detection"; and "analyse links… to reveal hidden connections… and communication patterns".[18] The Director of Public Prosecutions has commissioned a pilot of "true artificial intelligence" in the "search and analysis of mobile phone downloads" and "identifying the relevance of material".[19]

Neither the police nor the CPS should be outsourcing such extremely sensitive tasks to an experimental computer system that automates data processing, obstructs accountability and transparency, and could allow for even more disproportionate intrusions of privacy. It is unclear whether complainants are specifically informed of the use of such technologies or given the opportunity to explicitly consent to their use. There is a significant risk that such automated processing could constitute profiling, engaging Article 22 GDPR.

'Stafford' or consent statements and disclosure of complainants' information

The Criminal Procedure and Investigations Act 1996 and accompanying policy and guidance[20] sets out a duty on prosecutors to disclose certain information to the defence that they hold as a result of the police's investigation of an alleged crime, including information on victims of crime – complainants.

---

12 Dame Vera Baird QC, PCC for Northumbria, 'Letter to Justice Committee', 14 February 2018 (http://www.apccs.police.uk/wp-content/uploads/2016/11/Letter-to-Justice-Committee-Chair-regarding-disclosure-in-criminal-cases-140218.pdf)
13 Dame Vera Baird QC, PCC for Northumbria, 'Letter to Justice Committee', 14 February 2018 (http://www.apccs.police.uk/wp-content/uploads/2016/11/Letter-to-Justice-Committee-Chair-regarding-disclosure-in-criminal-cases-140218.pdf)
14 The Angiolini Review noted that the CPS "consistently reject [case] files due to the absence of key information such as…. social media, and third party material including social services records". 'Angiolini Review', 2015, para 518
15'Angiolini Review', 2015, para 518
16 https://www.theguardian.com/uk-news/2018/may/27/police-trial-ai-software-to-help-process-mobile-phone-evidence
17 https://www.theguardian.com/uk-news/2018/may/27/police-trial-ai-software-to-help-process-mobile-phone-evidence
18 https://www.cellebrite.com/en/products/analytics-enterprise/
19 http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/justice-committee/disclosure-of-evidence-in-criminal-cases/written/86396.pdf
20 The CPIA Code of Practice, Attorney General's Guidelines on Disclosure and Supplementary Guidelines on Digitally Stored Material 2013, CPS Disclosure Manual, CPS Rape and Sexual Offences Guidance

However, there are no safeguards to protection victims in the investigation or disclosure stages. Especially where the police's initial collection of information about a complainant's private life is disproportionate, as described above, disclosure can result in complainants' personal and sensitive information being disclosed to the defendant.

The Attorney General's Guidelines on Disclosure 2013 and the Supplementary Guidelines on Digitally Stored Material contain no safeguards or protections for complainants against such overly intrusive investigations or subsequent disclosure, other than general statements and obligations on the defence.[21] The ability to disclose complainants' personal information is derived from the complainant's 'consent'.

Complainants are pressured into consenting to the disclosure of their personal information by a broad and all-encompassing consent form known as a 'consent' statement or 'Stafford' statement.[22] 'Stafford' statements are presented to the complainant as an additional witness statement or a 'consent form',[23] in such a way that they not be fully aware of what they are consenting to, and that may prevent due consideration being given to their data protection rights. It is unclear whether the complainant could feasibly withdraw consent to disclosure of their personal information. Dame Vera Baird QC has expressed fears that such consent statements may not be read thoroughly, resulting in complainants unknowingly restricting their ability to exercise their Article 8 rights.[24]

These 'consent' or 'Stafford' statements are so broadly worded as to allow for the disclosure of all or any material collected as part of the case, with blanket provisions in relation to certain types of material, such as "Material held by the local authorities", "School/Education records", "Any counselling records", "Medical and any psychiatric records".[25] Clearly, the consent sought is not specified but rather is as enabling as possible, undermining the complainant's data protection and privacy rights.

The Crown Prosecution Service's Rape and Sexual Offences Guidance does indeed note that the "the prosecutor should take account of the article 8 ECHR rights of the person to whom confidential material relates" and that the "prosecutor must be satisfied that the person to whom the material relates consents to such disclosure." [26] However, if consent is given via one of these statements, there is no requirement for a hearing to consider the complainant's Article 8 rights and therefore the

---

21Attorney General's Office, 'Attorney General's Guidelines on Disclosure' December 2013, Annex para A3(b) (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/262994/AG_Disclosure_Guidelines_-_December_2013.pdf)

22Following *R (B) v Stafford Crown Court* [2007] 1 All ER, a complainant's Article 8 rights must be considered when it comes to disclosure.

23Dame Vera Baird QC, PCC for Northumbria, 'Letter to Justice Committee', 14 February 2018 (http://www.apccs.police.uk/wp-content/uploads/2016/11/Letter-to-Justice-Committee-Chair-regarding-disclosure-in-criminal-cases-140218.pdf). A 'Witness Statement' consenting to disclosure is attached as an annex to this evidence.

24Dame Vera Baird QC, PCC for Northumbria, 'Letter to Justice Committee', 14 February 2018 (http://www.apccs.police.uk/wp-content/uploads/2016/11/Letter-to-Justice-Committee-Chair-regarding-disclosure-in-criminal-cases-140218.pdf)

25'Witness Statement MG11 'Stafford Statement' (Appendix4)

26CPS, 'Rape and Sexual Offences Guidance, Chapter 15: Disclosure and Third Party Material'. Available: https://www.cps.gov.uk/legal-guidance/rape-and-sexual-offences-chapter-15-disclosure-and-third-party-material

complainant is prevented from making representations about the disclosure as per *Stafford*[27]. The APCC has also warned that "In signing the statement complainants may be precluding any practical consideration of their Article 8 rights."[28]

Broad 'Stafford statements' put undue pressure on the complainant to consent to the disclosure, leaving complainants in a catch-22 situation: if they consent, deeply sensitive and personal details of dubious relevance to the case may be examined in court in an attempt to discredit them. If they do not consent, the case may not proceed to trial – a consequence which is emphasised by the police and the CPS in the 'Digital Processing Notice' and the 'consent' or 'Stafford' statements, respectively. Therefore, it cannot be considered that such blanket consent is in fact "freely given" as required by law.

This current practice appears to be at odds with what little the current policy has to say in relation to such overly-intrusive and disproportionate information gathering and disclosure. The Attorney General's Guidelines on Disclosure state that "Disclosure must not be an open-ended trawl of unused material" and that the defence must indicate what material is relevant,[29] while the Supplementary Guidelines on Digitally Stored Material specify that the defence must play a role and define the scope of digital material that might be necessary in the case.[30]

The law and policy in this area is clearly not up to date to deal with the availability of such large amounts of sensitive and personal information, meaning complainant's data protection and privacy rights are not being upheld in this most crucial context.

An important safeguard against such questionable disclosure practice is for police not to collect irrelevant personal information about complainants in the first place, and for complainant's data protection rights to be respected throughout the entire investigative and disclosure process.

Conclusion

The current consent procedures for the collection, analysis and disclosure of complainants' personal information appears to lack the critical features required by law, notably the GDPR. Firstly, consent cannot be considered to be "freely given" in current practices due to the imbalanced relationship between the complainant and police, the likelihood of trauma, and complainants' competing considerations such as justice and public safety. Secondly, the consent is not specific, but rather performs as a catch-all abdication of data protection rights and the Article 8 right to privacy. Thirdly,

---

27 *R (B) v Stafford Crown Court* [2007] 1 All ER
28 APCC calls for inquiry to look at all sides of disclosure – APCC, 14 February 2018: http://www.apccs.police.uk/latest_news/apcc-calls-inquiry-look-sides-disclosure/
29 Attorney General's Office, 'Attorney General's Guidelines on Disclosure' December 2013, para 9 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/262994/AG_Disclosure_Guidelines_-_December_2013.pdf)
30 Attorney General's Office, 'Attorney General's Guidelines on Disclosure' December 2013, Annex para A3(b) (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/262994/AG_Disclosure_Guidelines_-_December_2013.pdf)

consent may not be fully informed because complainants would not reasonably expect the sheer scale of data seizure and examination into their private lives or the complex legal and practical implications that could arise in the course of the investigation and trial.

It would be possible for complainants to freely give specific, informed consent in relation to specific pieces of information – but that is far from current practice. Where police wish to investigate further reasonable lines of inquiry, they should ask the complainant for access to further specified pieces of information, which they could freely choose whether or not to consent to. However, if police wish to effectively investigate a complainant – for example, to investigate whether the complainant is making a false allegation – then consent is an inappropriate mechanism by which to access such personal information.

We are aware that the Victims Commissioner has written to you about Stafford statements. We support an investigation into the use of these statements and the issue of consent within sexual violence investigations and cases. However, we believe the protection of data pertaining to complainants of sexual violence must be examined holistically, from the initial police investigation and the personal data the police transfer to the CPS, through to subsequent disclosure by the CPS to the defence.

We believe that this issue is extremely significant and therefore merits a prioritised investigation.

Yours sincerely,

Silkie Carlo

Encl.

cc. Centre for Womens Justice

Appendix

1. Metropolitan Police: Overview Statement
2. Metropolitan Police: 'Digital Processing Notice'
3. Metropolitan Police: 'Digital Device Downloads – information for complainants and witnesses'
4. 'Witness Statement MG 11' 'Stafford Statement' part 1 and part 2