Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

The Information Commissioner's Response to consultation on the Attorney General's Guidelines on Disclosure and the CPIA Code of Practice

The Information Commissioner is responsible for promoting and enforcing data protection law in the UK including the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018). She is independent of government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. She does this by providing guidance to individuals and organisations, solving problems where she can, and taking appropriate action where the law is broken.

The Information Commissioner's Office (ICO) recently published the report[1] ("our report") of its investigation into the practices used by police forces in England and Wales when extracting data from mobile phones in the context of criminal investigations. In addition, the ICO has a separate ongoing investigation looking more broadly into the path that victims' data takes through the criminal justice system from allegation, through disclosure, prosecution and compensation.

There are opportunities to reinforce data protection rights through revisions to the Attorney General's Guidelines on Disclosure ("the AG Guidelines") and the CPIA Code of Practice ("the CPIA Code"), and this was a key recommendation arising from our investigation.

In addition, the ICO conducts criminal investigations in its own right into potential breaches of data protection law and is subject to the CPIA and Disclosure Guidelines.

Further, the Information Commissioner, as part of her powers to take enforcement action under the GDPR and the DPA 2018, has the discretion to investigate and prosecute, if appropriate, criminal offences under this legislation. The ICO therefore recognises the challenges and complexity of the disclosure regime and welcomes the opportunity to respond to this consultation.

[1] https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf

Background

Our report sets out the nature of the digital materials held on mobile phones as being deeply personal in nature, including innermost thoughts, relationships, health and finances, and potentially relating to a large number of individuals. This means that, under the DPA 2018, any form of processing of this material amounts to "sensitive processing"[2] for a law enforcement purpose, and therefore is subject to more stricter conditions than would otherwise be the case in order for the processing to be lawful. It is important to recognise that "processing" includes a range of actions from the initial acquisition to its eventual destruction, including (most notably for this consultation) disclosure by transmission, dissemination or otherwise making available, and restriction, erasure or destruction[3].

For clarity, we draw a distinction between the term "sensitive" as used in the context of disclosure and that defined in the DPA 2018.

It would be helpful for section 2 of the Code to include a definition of 'unused material'.

Reasonable lines of inquiry

Our investigation found inconsistent practice in the application of the obligation in the CPIA to pursue all reasonable lines of inquiry (RLOIs), whether they point towards or away from the suspect. We acknowledge the challenges that may lead to this inconsistency, including the need to consider the lines of enquiry on a case-by-case basis, and that, at an early stage of an investigation, it may not be clear whether an offence has been committed or whether material obtained may be evidential or unused. We also acknowledge that RLOIs may evolve as an investigation progresses.

While acknowledging these challenges, we are concerned that there may be excessive processing of sensitive data when this is not based on a RLOI. Our report explains how, often, more material is obtained than may be relevant to the specifics of a case.

The focus of this particular consultation appears to be around the appropriate handling of relevant material already obtained. Our concern is in all aspects of processing, including the basis for obtaining the material and storing it, in addition to disclosing it. It

[2] Section 38(8) DPA 2018
[3] Section 3(4) DPA 2018

would therefore be helpful if both the Guidelines and the Code gave greater consideration to RLOI and the obligation, under data protection law, for personal data being processed to be adequate, relevant and not excessive[4].

The Guidelines and Code are silent on the issue of the handling of non-relevant materials. This is a matter of considerable concern to the ICO and was a key factor discussed in our report. Whilst the ideal position would be that only relevant material is handled by investigators, it is often the case, particularly with digital materials, that an investigation will collect a far greater volume of non-relevant data than that which is potentially relevant to the case, and, as outlined above, this material may be highly intrusive into the lives of third parties who are not relevant to the investigation, some of whom may be children or other vulnerable persons. The Guidelines and Code should emphasise the obligation to avoid, to the greatest extent possible, the obtaining of non-relevant material and, where it is unavoidably obtained, how it must be safeguarded and processing ceased at the earliest opportunity.

Where paragraph 21 of the Guidelines states that the assessment of relevance "requires an exercise of judgement", it would be helpful if this was expanded upon to state the requirement for critical consideration and respect for privacy.

In the discussion in Annex B of the Guidelines, in relation to pre-charge engagement, it is suggested that this should take place in only a minority of cases. We would advocate this engagement at the earliest possible opportunity, in order to inform RLOI that are more appropriately defined. We do, however, recognise the challenges that exist with this, including reliance upon the co-operation of the suspect and their legal representatives.

The particular nature of electronic material

We are concerned about the significant adverse effects inappropriate collection and disclosure of sensitive personal data can have on victims[5] in particular, and the potential for this to undermine criminal justice processes. The lack of confidence felt by victims when handing over devices containing highly intrusive personal data about themselves,

[4] Section 37 DPA 2018
[5] Here, we use the term 'victim' in recognition of the trauma that may have already been experienced in the context of a violent offence.

their friends and families, is widely documented[6]. Of particular concern is the collection of data from a victim's phone as a result of a disproportionate lines of inquiry, for example unduly focusing on a victim's good character being a key factor examined in making a charging decision. It would be helpful for the section of the Guidelines on "Electronic material" to reflect the unique nature of electronic devices and the insights they provide into private lives. Specifically, we would request that it is explicitly referenced that the data on a phone is likely to be special category and therefore the sensitive processing element must be reflected, and also that the data on the phone does not belong to the phone's owner or user; it is likely to relate to many data subjects.

Paragraph 11 of the Guidelines refers to balancing the right to a fair trial and the privacy rights of victims and witnesses. The Court of Appeal (Civil Division) has reiterated that a suspect also has a reasonable expectation of privacy in relation to the fact and details of a criminal investigation into his or her activities, until the point of charge. Our report goes further to emphasise that, particularly in relation to digital materials, it is also important to consider that all persons have privacy rights, including those not involved in the investigation but whose private lives may be impacted upon through collateral intrusion.

Paragraph 43 of the Guidelines refers to the extent and manner of examination being "appropriate" to the issues in the case. They should also be proportionate and be reflective of the intrusion into the privacy of those whose data is contained within the material.

Paragraph 44 of the Guidelines states the obligation to return devices at the earliest opportunity after it has become apparent that they do not contain relevant material. This is clearly helpful, but it focuses on the physical device rather than its contents. It should also be stated that any copies of non-relevant material should be permanently deleted at the same time.

Management of electronic material

Our report documents concerns about the handling of electronic material when in the possession of the police (and possibly others) during the criminal justice process.

[6] See, for example, https://www.london.gov.uk/sites/default/files/vcl_rape_review_-_final_-_31st_july_2019.pdf

We welcome the recognition of difficulties faced by investigators with large volumes of digital data and the scheduling of that material. The digital disclosure strategy plays an increasingly important role in the investigative process, and it is therefore helpful to see the encouragement of appropriate investment in digital forensic expertise reflected in the consultation.

In the "Retention" section of Annex A of the Guidelines, it would be helpful to have reference to an obligation to retain material in a way that facilitates its management (retention, review, deletion) in order to be compliant. A key concern for us is the problem of digital forensic assets not being managed consistently with the progression of the case, with the risk that they are not disposed of at the appropriate time.

The same section makes a number of references to "inextricably linked non-relevant material" and cross-refers to PACE Code B. This appears to relate mainly to physical devices but, in any event, would benefit from further clarification. In the case of a mobile phone, it is accepted that an investigator may need to take possession of the device in order to be able to extract relevant material. For example, it could be argued that the material is inextricably linked whilst locked within the device but, once it has been extracted, non-relevant data could (and we would argue should) then be deleted.

Both the Guidelines and the Code could be clearer in terms of drawing the distinction between the management of physical artefacts and the digital material obtained from their examination. A case in point is paragraph 24 of Annex A of the Guidelines, where there is reference to material being 'returned'. However, data protection legislation is equally concerned with copies of material rather than just the original source.

We respect the need to adhere to the principle of best evidence in order to assure the integrity of material. Adopting the standards mandated by the Forensic Science Regulator should provide a measure of assurance in this regard in relation to material acquired from source devices. However, to accommodate cases where it is not possible to separate and dispose of what is not considered to be relevant, the Guidelines could be strengthened to better reflect the highly sensitive nature of the data obtained from electronic devices and the requirement to manage all personal data in accordance with the DPA 2018.

Section 5 of the Code sets out obligations regarding the retention of material. It would be helpful if this section also referenced the duty to comply with data protection legislation, particularly in relation to the obligation to periodically review the requirement to retain the material and to retain it for no longer than necessary[7]. The requirement to retain material for a minimum period should not be interpreted as justifying long-term or unmanaged retention.

The rebuttal presumption

The list of material that can be subject to the rebuttable presumption and therefore be likely to meet the test for disclosure (set out in paragraph 18 of the consultation document and paragraph 74 of the Guidelines) appears appropriate.

Timing of revelation

We agree with the principle that disclosure should be carried out at the earliest stage possible. Paragraph 32 of the consultation document makes reference to recognition of the practical challenges associated with providing unused material schedules prior to charge or at the point of charge. We believe this is particularly the case when dealing with increasingly large numbers of digital devices and exponentially growing amounts of digital data. This underlines our concerns around potentially excessive processing of data and amplifies the requirement for effective management of data extracted from devices.

[7] Section 39 DPA 2018