Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524510 www.ico.gov.uk

Rt Hon Harriet Harman QC MP
Joint Committee on Human Rights
Houses of Parliament
London
SW1A 0AA

17 May 2021

Dear Ms Harman,

Re: Legislative Scrutiny of the Policing, Crime, Sentencing and Courts Bill

Does the power to extract information from electronic devices set out in Chapter 3 of Part 2 of the Bill comply with the right to respect for private life (Article 8 ECHR)?

Background

The Information Commissioner is responsible for promoting and enforcing data protection law in the UK, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA). 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.

In June 2020, the Information Commissioner's Office (ICO) published a report[1] 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. It reflected the diminishing confidence victims, in particular of serious sexual crimes, have in coming forward and being assured that they will

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

be treated with dignity and without undue intrusion into the most intimate aspects of their lives and the lives of others.

Mobile phones and other electronic devices have become ubiquitous parts of citizens' lives. They are constantly generating and storing data that, when examined, can reveal private communications, photos, videos, locations visited, personal preferences, and much more. The user of the device and those they communicate with will have a reasonable expectation that this data will be kept private and secure.

The ICO found that police forces are often unclear about the lawful basis for their first obtaining mobile devices and then extracting data from them. Police data extraction practices vary across the country, with excessive amounts of personal data often being extracted, stored, and made available to others, without an appropriate basis in data protection law.

The criminal justice and data protection law applicable to this area is complex, and there exist a wide range of powers available to police officers and other authorised persons. However, people expect to understand how their personal data is being used, regardless of the legal basis for processing. The ICO therefore called for the introduction of an overarching statutory code of practice that governs the extraction of information and provides a framework assisting officers to understand the approach to be taken in obtaining and processing data from a device. The code of practice should cover all cases where data might be extracted, rather than just the specific circumstances or under specific powers as currently provided for in the Bill.

Summary

As currently drafted, the powers set out in Chapter 3 of Part 2 of the Bill are unlikely to comply with Article 8 of the ECHR, as they allow for an interference with the rights of individuals without satisfying the necessary legal prerequisites to do so. Therefore, they may be open to legal challenge. Further, the Bill could undermine the protections offered to third parties by existing legislation. It risks dissuading citizens from reporting crime, and victims and witnesses may be deterred from assisting police.

Concerns

In seeking to empower victims and witnesses to come forward and seek justice, care must be taken to ensure there is no unintended consequential impact on the rights of others.

The power proposed in s36 of the Bill refers to a user of the device having "voluntarily provided" and "agreed to" the extraction of information from the device. These terms align with the concept of consent in data protection legislation.

The ICO's investigation found that the conditions required under Article 7 UK GDPR for consent to be valid are unlikely to be met in the context of a person agreeing to the extraction of data from their device. More fundamentally, the agreement of a user of a device is not an appropriate or sufficient basis for a power that results in the processing of sensitive personal data which provides a detailed insight into the lives of many people who would have a reasonable expectation of their data being kept private. In other words, a person cannot waive the Article 8 ECHR right of other persons. More significantly from the ICO's regulatory remit, a victim or a witness is not able to erode the information rights offered to all persons under the DPA.

The ICO investigation found that examination of an electronic device containing sensitive personal data must:

- be based on a reasonable line of enquiry;
- only be carried out when other, less intrusive means of addressing the enquiry have been considered; and
- be limited to the material strictly necessary.

These findings were reflected in the updates the Attorney General's Guidelines on Disclosure[2], the Criminal Procedure and Investigations Act 1996 (section 23(1)) Code of Practice[3], and considered by the Court of Appeal judgment in the case of Bater-James & Anor v R [2020] EWCA Crim 790[4].

The Bill, as currently drafted, makes no reference to reasonable lines of enquiry, nor does it limit the extent of the extraction of information to that which is strictly necessary. There is a risk that all available data will be taken from the device, and the condition at s36(7)(b) of it not being "reasonably practicable" to use other means is not articulated with sufficient clarity to be of assistance to those using the powers or scrutinising their use.

Bank Mellat v Her Majesty's Treasury (No. 2) [2013] UKSC 39[5] asserted the importance of weighing a measure's effects on the rights of the persons to whom it applies against the importance of the objective of the measure. There appears to be insufficient consideration of this test in the conditions associated with the proposed powers. This calls into question the extent to which exercising these powers will meet the s35(2) DPA requirement for processing to be "based on law".

---

2 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946082/Attorney_General_s_Guidelines_2020_FINAL_Effective_31Dec2020.pdf

3 https://www.gov.uk/government/publications/criminal-procedure-and-investigations-act-1996-section-231-code-of-practice

4 http://www.bailii.org/ew/cases/EWCA/Crim/2020/790.html

5 https://www.bailii.org/uk/cases/UKSC/2013/39.html

The ICO's finding that the exercising of powers needs to be based on strict necessity and proportionality, predicated on a definable investigation, has been overlooked in the drafting of the powers. The problem with a consent-based approach in the proposed new powers is self-evident. There is no stipulation of what information must be given to a user about the extraction of information, under s36(1)(b) of the Bill, for 'agreement' to be sufficient, nor is it clear when, if at all, the user is able to withdraw their consent. It is questionable how freely consent is given, if a user is informed that their other rights (e.g. Article 2 or 3 ECHR) may not be protected by a prosecution if they fail to provide that consent. A new code of practice would have to deal with such issues, but this reliance on the consent of the user is likely to remain a key flaw in the new power as it is used in practice.

It is acknowledged that the Bill requires a code of practice be produced to provide guidance about the exercise of the proposed powers. However, what is required is a code of practice that governs the practice of data extraction in all circumstances, not just those where one of the new powers is being exercised.

The existence of a code of practice is not simply a helpful guide to those exercising the new powers. It will be critical to ensuring that the legal provisions have sufficient specificity and contain adequate safeguards to be "in accordance with the law" and thereby compliant with Article 8(2) ECHR. In the absence of such additional explanatory guidance on the new power itself, we are not satisfied that this fundamental requirement of legality will be met.

The ICO investigation identified significant concerns with the use of existing powers in relation to privacy issues arising from the extraction of data from devices belonging to victims, witnesses and suspects. The majority of extractions involve devices taken from suspects, which are beyond the scope of this Bill. The proposals do nothing to address the current privacy rights issues associated with such processing, and introduce new powers with insufficient safeguards. There is a significant risk that existing poor practice may continue unabated.

Conclusions

The proposed powers set out in Chapter 3 of Part 2 of the Bill do not address the concerns set out in the ICO report and add to an already complex range of legislation and related powers. If any new powers are introduced, they need to be accompanied by appropriately robust safeguards around their use, and these safeguards must have applicability regardless of the mode of engagement with the citizen. The rights in data protection legislation of the many persons whose data is held on a device need to be afforded the same level of protection regardless of the circumstances under which the device is obtained. As such, there is a significant risk of these new powers being incompatible with Article 8 ECHR, and the potential for the privacy and information rights safeguards offered by data protection legislation to be undermined is concerning.

The ICO's report recommended the introduction of an overarching code of practice that governs extractions by authorised persons and ensures due consideration of privacy and information rights in all circumstances of engagement with individuals, regardless of whether an individual has agreed to provide their device.

Yours Sincerely,

Information Commissioner's Office