PRIVACY INTERNATIONAL'S SUBMISSION TO THE JOINT COMMITTEE ON HUMAN RIGHTS ON THE DRAFT POLICE, CRIME, SENTENCING AND COURTS BILL 2021

Compliance of Chapter 3 of Part 2 of the PCSC Bill with the right to respect for private life (Article 8 ECHR)

14 May 2021

Submitted to the Honourable Members of the Joint Committee on Human Rights

Table of Contents

Introduction *2*

Summary of key concerns 2

Background to PI expertise in this area *2*

PI's concerns regarding scope of 'electronic device' *4*

PI's concerns regarding extraction of information from electronic devices *5*

Problems surrounding reliance on consent to extract data from electronic devices *6*

What is the alternative? 7

The Bill fails to provide safeguards to ensure that the gathering of data from electronic devices is proportionate and strictly necessary for the investigation in question *8*

The definition of 'authorised persons' is too broad. *10*

Failure to provide for adequate oversight, notification and redress mechanisms *10*

Annex 1: What is needed to inform an individual (non-exhaustive list) *12*

Extraction: 12

Examination: 12

Disclosure: 12

Privacy International ("PI") was founded in 1990 and is based in London, UK. It was the first organization to campaign at an international level on privacy issues. It is committed to protecting people's privacy, dignity and freedoms from abuses by companies and governments. Through research, litigation and advocacy, it works to build a better future where technologies, laws, and policies contain modern safeguards to protect people and their data from exploitation.

Introduction

1. Thank you for the opportunity to provide comments on the draft Police, Crime, Sentencing and Courts Bill ("PCSC") Bill 2021.

2. We respond to the first question - whether the power to extract information from electronic devices set out in Chapter 3 of Part 2 of the PCSC Bill comply with the right to respect for private life (Article 8 ECHR).

3. PI's analysis of the Chapter 3 of Part 2 of the draft PCSC Bill demonstrates numerous failures to safeguard individuals' privacy. As a result, we believe that the Bill in its current form cannot comply with the right respect for private life under Article 8 ECHR.

Summary of key concerns

a. **The breadth of definition of electronic devices.**
b. **Lack of clarity on powers of seizure.**
c. **Reliance upon voluntary provision of an electronic device fails to appreciate the inherent power imbalance between the police and individuals.**
d. **Reliance upon agreement to extraction of data from that device fails to account for the breadth of data which can be obtained and the likelihood an individual will have little understanding of either the volume or how it can be processed using for example, artificial intelligence tools.**
e. **The use of cloud extraction.**

Background to PI expertise in this area

4. In April 2018, following PI's ground-breaking research into mobile phone extraction, PI published its 'Digital Stop and Search Report'[1] and made a complaint to the Information Commissioner's Office[2] ("ICO") in relation to the use of mobile phone extraction ("MPE") technology by police forces. These highlighted issues surrounding the use of MPE, including the lack of legal basis, safeguards and independent oversight for this power.

[1] Privacy International, Digital Stop and Search Report (March 2018) available at: https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf
[2] Privacy International, Complaint to the ICO (April 2018) available at: https://privacyinternational.org/sites/default/files/2018-04/Complaint%20to%20ICO%20about%20Mobile%20Phone%20Extraction%2026th%20April%202018.pdf

5. In June 2020, responding to PI's complaint, the ICO released its critical report[3] on the use of MPE technology. The ICO called for reforms and safeguards to protect an individual's data from unnecessarily intrusive practices. The ICO echoed PI's concerns that currently, there is no clear legal basis, policy guidance or independent, effective oversight for police forces' use of MPE technology.

6. We suggest the lack of clear legal basis should be borne in mind when considering the purpose of the government's proposals in Chapter 3 Part 2 of the Bill.

7. PI were also involved in extensive engagement with Police Scotland regarding the legality of the roll out of mobile phone extraction kiosks[4].

8. PI has raised concerns including with the Investigatory Powers Commissioner[5], about whether in some, or indeed in all circumstances, the use of MPE technology constitutes either an interception of communications or 'equipment interference' (i.e. hacking).[6] In *Liberty and Others v United Kingdom,* the ECtHR reiterated that the mere existence of powers "permitting the examination, use and storage of intercepted communications constituted an interference with the Article 8 rights".[7]

9. PI has written at length on how we believe the technology operates, which at times has not aligned to what is stated as possible or not possible by law enforcement and governments. We can assist the Committee further on these issues if required.

10. The PCSC Bill aims to introduce a new statutory power enabling the police to obtain digital evidence from devices, providing safeguards are followed, and ensuring that only the relevant information is taken.[8] We find instead that it is particularly scant on these areas. PI's analysis of the Chapter 3 of Part 2 of the draft PCSC Bill demonstrates numerous failures to safeguard

---

[3] ICO, Investigation Report: Mobile Phone Data Extraction by Police Forces in England and Wales (June 2020) available at: https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf

[4] Privacy International, Old Law, New Tech and Continued Opacity: Police Scotland's use of Mobile Phone Extraction (12 September 2019) available at: https://privacyinternational.org/report/3202/old-law-new-tech-and-continue-opacity-police-scotlands-use-mobile-phone-extraction See also Privacy International, Submission to Police Scotland on Cyber Kiosks 10 March 2020 available at: https://privacyinternational.org/node/3394

[5] Privacy International, Submission to IPCO on the Digital Stop and Search Report, 1 August 2018, available at: https://privacyinternational.org/sites/default/files/2018-08/IPCO%20letter%20Police%20MPE.pdf

[6] Ibid.

[7] *Liberty and others v UK*, (No. 58243/00, 1 July 2008) para 57

[8] Police, Crime, Sentencing and Courts Bill 2021: data extraction factsheet, available at: https://www.gov.uk/government/publications/police-crime-sentencing-and-courts-bill-2021-factsheets/police-crime-sentencing-and-courts-bill-2021-data-extraction-factsheet

individuals' privacy. As a result, we believe that the Bill in its' current form cannot comply with the right respect for private life under Article 8 ECHR.

11. We are concerned that the powers in the draft PCSC Bill are an attempt to avoid dealing with the real and recognised issues concerning the lack of, or, inadequate legal basis upon which to seize electronic devices. Section 36(9) of the PCSC Bill states that "this section does not affect any power relating to the extraction or production of information, or any power to seize any item or obtain any information, conferred by an enactment or rule of law." This begs the question, what powers are they referring to.

12. We urge the Committee to question the Government why they appear to be creating a problematic workaround in the PCSC Bill which enables them to extract data from electronic devices, avoiding the creation of a legal framework that is publicly accessible, clear, precise, comprehensive and non-discriminatory.

13. We reiterate that PI has repeatedly stated that a warrant should be obtained in order to seize and examine electronic devices. The requirement of a warrant would ensure independent oversight into what data is examined and provide a layer of protection to ensure that it is only that which is strictly necessary.

PI's concerns regarding scope of 'electronic device'

14. Chapter 3 concerns the 'Extraction of Information from Electronic Devices'. Much of the focus has been on mobile phones. However, electronic devices are not sufficiently defined[9] or elaborated upon.

15. The Committee must consider the implications, for example, of exploiting connected devices or what are known as 'internet of things' such as an Amazon Echo, Google Home, Fitbit, connected toys, smart TV, smart fridge and the plethora of other devices that could fall under this term. Whilst an individual may understand that their phone holds relevant messages, it is questionable what an individual may understand is held on an internet of things device and what can be obtained from extracting this data. Legal mechanisms are in place for law enforcement to approach the relevant company to obtain cloud stored data.

[9] Section 36(10) Police, Crime, Sentencing and Courts Bill 2021 provides that "electronic device" means any device on which information is capable of being stored electronically and includes any component of such a device.

16. This raises new challenges and risks that have not been sufficiently explored.[10] There has been no consideration as to how these devices differ from mobile phones. If the Committee seeks elaboration on this point, we can provide further information.

PI's concerns regarding extraction of information from electronic devices

17. Use of MPE to obtain digital evidence is highly intrusive and relates not just to the data of the user of the phone but also those of the many other people who have communicated with the user.

18. Extraction technology[11] allows access to vast quantities of data stored on individual's mobile phone for download and storage, from the expected such as call logs and messages, to the unexpected - including deleted data[12], Wi-Fi connections, voice requests to Alexa or Siri stretching back many years. This can include contacts, messages, web browsing history, health data and banking information.

19. We highlight to the Committee the increasing propensity and popularity of tools which download data stored in the Cloud[13]. Cloud extraction is the ability to access, extract, analyse and retain data stored in the Cloud such as on third party servers. This may include data from numerous platforms such as Facebook, Twitter, Instagram and related to products such as Dropbox, Slack and Uber.

20. Cloud extraction provides access to not just what is contained on the phone, but also to what is accessible from it. We have written about this extensively and can provide further information.

---

[10] Privacy International, Response to documents disclosed in advance of External Reference Group meeting which took place 21st November 2019, paras 152-157, available at: https://privacyinternational.org/sites/default/files/2020-01/External%20Reference%20Group%20submissions%20December%202019%20FINAL.pdf, See also Privacy International, With My Fridge As My Witness, June 2019 available at: https://privacyinternational.org/long-read/3026/my-fridge-my-witness

[11] Privacy International, A Technical Look at Phone Extraction, 14 October 2019, available at: https://privacyinternational.org/long-read/3256/technical-look-phone-extraction

[12] Privacy International, Push this Button for Evidence, 16 May 2019 available at: https://privacyinternational.org/news-analysis/2901/push-button-evidence

[13] Privacy International, Cloud Extraction Technology: the secret tech that lets government agencies collect masses of data from your apps, 7 January 2020 available at: https://privacyinternational.org/long-read/3300/cloud-extraction-technology-secret-tech-lets-government-agencies-collect-masses-data

Problems surrounding reliance on voluntary provision and agreement to extract data from electronic devices

21. Section 36 of the PCSC Bill provides that an authorised person, such as a police officer, can extract data from an electronic device if the user of a device has:
    a) voluntarily provided it, and;
    b) has agreed to the extraction of data from that device.

22. We understand the PCSC Bill does not rely upon consent pursuant to Article 4(11) GDPR to seize and extract a user's data. The PCSC Bill will permit seizure of a device and extraction of information if the device is provided voluntarily and with the user's agreement.

23. Given the inherent power imbalance between the police and the user, the instances in which provision of a device will be truly voluntary is questionable, making it an unstable basis upon which to legally seize a device.

24. The ICO states in their report that individuals may be worried that a decision not to consent will impact on the progress of their case, especially when the electronic devices are taken from victims of rape and sexual assault.[14]

25. Further, the owner of the device cannot provide consent on behalf of all others whose data is stored on their device, such as family and friends.[15]

26. The Bill is silent on the ability of the individual to withdraw their consent to the provision of their device i.e., request its return and whether an individual can cease their agreement to the gathering and storage of their data.

27. If individual 'voluntarily' provides the device, they should be able to change their mind and request that any extracted data is deleted. However, it appears from the Bill that once initial agreement is given to take possession of the phone and extract data from it, there is no way of going back. Considering the problems identified above, PI is very concerned that the new statutory measure rests solely on this concept.

28. The lack of information provided to the individual regarding extraction, examination, retention, deletion, sharing and search parameters

[14] Information Commissioner's Office, Investigation Report: Mobile Phone Data Extraction by Police Forces in England and Wales (June 2020) p 36 available at: https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf
[15] *Ibid*, pp 15-16.

undermines that any seizure or provision which is for the purpose of examination can be informed or agreed to.

29. An individual will not be aware when making the agreement whether for example search parameters will apply to extracted data to protect a victim's rights. An individual will be unaware if advanced machine learning technology will be used to analyse data extracted from the Cloud. We set out in Annex 1, a non-exhaustive list of information that should be provided to an individual.

30. We further question, if individuals are not provided with legal advice or other independent support in reaching a decision regarding provision of their electronic devices, and since they are likely to be in a state of distress, whether they can truly have capacity to make an informed decision free from pressure and influence.

31. The use of 'voluntary provision' and 'agreement' gives the illusion of empowering individuals, when in reality, withdrawal of agreement may have little or no impact.

32. We highlight to the Committee that consideration needs to be given to the implications of extracting legally privileged and journalistic information.

What is the alternative?

33. We submit that consent or 'voluntary provision' should not be the basis for the legal measure granting powers to seize the device, nor agreement the basis for legal measures granting powers to extract data from electronic devices.

34. The government must provide a legal framework for seizure of the device and extraction of data that is publicly accessible, clear, precise, comprehensive and non-discriminatory. They must address the concerns raised by the ICO.

35. A list of targeted criteria should be identified to which authorised persons should comply before electronic devices are seized and data is extracted. This list of targeted criteria needs to include the following, by way of example:
    a) a reasonable suspicion that the device contains material evidence necessary for the investigation in question
    b) other practical steps have been taken to obtain this information but have not been successful

c) the information extracted will pursue clear lines of enquiry and be limited to specific data necessary for the investigation
d) independent authorisation for extraction of information from that device must be obtained
e) the user of the device has been notified of the intention to extract limited and specific data from their device and what data will be extracted
f) The electronic devices must not be kept longer than necessary and should be returned within 30 working days.

36. The ECtHR in *Gillan and Quinton v UK*[16] and *S and Marper v UK*[17] continuously expressed concerns over an intrusive power that did not did not require any "reasonable suspicion". The same reasoning applies to extraction of data from electronic devices in the draft PCSC Bill. In order to comply with the Article 8 ECHR, extraction of data from electronic devices must not just depend on individual's agreement to this, but on an existence of reasonable suspicion that the device contains data relevant to the investigation in question.

The Bill fails to provide safeguards to ensure that the gathering of data from electronic devices is proportionate and strictly necessary for the investigation in question

37. The ICO report confirmed PI's concerns that the data extracted and processed from the mobile phones was often too excessive.[18] Despite the availability of privacy-enhancing functions in the software tools, police forces simply grabbed more data than necessary in the investigative

[16] *Gillan and Quinton v UK*, (No. 4158/05, 12 January 2010), para 85. In this case the power of random stop and search individuals under s44 of the Terrorism Act 2000. The court stated that such broad discretion gave rise to a "clear risk of arbitrariness"
[17] *S and Marper v UK* [GC], (No. 30562/04, 4 December 2008), para 135. In this case the Grand Chamber (ECtHR) held that the retention of DNA samples from people who had not been charged or convicted of a criminal offence was a "disproportionate interference" with those individuals' private lives.[17] Central to the reasoning was the absence of any assessment of suspicion by the authorities that was sufficient to justify the retention of each individual's DNA data. See also Catt v the United Kingdom (No. 43514/15, 24 January 2019) where the ECtHR found that the UK violated the right to privacy of Mr John Catt, a peace movement activist, who despite having never been convicted of any offence, had his name and other personal data included in a police database known as the "Extremism Database". The Court found problematic the "significant ambiguity over the criteria being used by the police to govern the collection of the data in question."
[18] Information Commissioner's Office, Investigation Report: Mobile Phone Data Extraction by Police Forces in England and Wales (June 2020) pp 44-46 available at: https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf

process.[19] In addition, the ICO report warned that the police cannot seize phones to go on fishing expeditions but must focus any extraction on clear lines of enquiry.[20]

38. Despite promising to provide sufficient safeguards and ensure that only relevant information is gathered[21], the draft PCSC Bill fails to do so. Section 36(6) and (7) simply state that if there is a risk of obtaining more information than necessary (which will exist every time a device is taken) the police forces will only need to consider if there are other ways to gather this information and if this would be practical to pursue. There is no consideration of limiting the extracted data or limiting the searches of that data.

39. We submit that the Bill therefore falls short of providing sufficient safeguards to ensure that authorised persons do not simply extract and retain disproportionate amount the data that is available on the device. It must include provisions setting out that only specific, limited amount of data relating to clear lines of enquiry should be gathered from devices. The ICO report confirmed that despite possibilities of MPE technology to minimise intrusion and maximise privacy of data, police forces simplified user interfaces, that did not allow for the use of privacy-enhancing functionality.[22] We therefore submit, that following extraction irrelevant data should be deleted immediately and searches of data restricted.

40. In order to comply with Article 8 ECHR independent authorisation must be put in place. The complete silence on these measures by the PCSC Bill is worrying considering the ICO report stated there were numerous security risks regarding how the police collected and stored the data from victims' and witnesses' mobile phones.[23] It found that the data obtained from individuals was not always categorised and kept together in bulk, leading to risks of serious compliance failures.

41. the UN Human Rights Committee recommended to the UK government in July 2015 to: "ensure that any interference with the right to privacy, family, home or correspondence is authorized by laws that: "are sufficiently precise and specify in detail the precise circumstances in which any such

[19] *Ibid.*, p 51.
[20] *Ibid,* p 39 and 46.
[21] Police, Crime, Sentencing and Courts Bill 2021: data extraction factsheet, available at: https://www.gov.uk/government/publications/police-crime-sentencing-and-courts-bill-2021-factsheets/police-crime-sentencing-and-courts-bill-2021-data-extraction-factsheet
[22] ICO, Investigation Report: Mobile Phone Data Extraction by Police Forces in England and Wales (June 2020) p. 51, available at: https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf
[23] *Ibid*. pp 47-48

interference may be permitted, the procedures for authorization…procedures for the use and storage of data collected".[24]

The definition of 'authorised persons' is too broad.

42. The list of 'authorised persons' in Schedule 3 of the PCSC Bill who can collect devices is very broad. It not only includes police officers and constables, but also 'employees of Common Council of the City of London', and immigration officers.

43. Including immigration officers is concerning, as the Bill could potentially lead to misuse of their powers enabling immigration officers to gather and analyse all devices from asylum seekers.

44. As currently drafted, the PCSC Bill can be interpreted to treat all asylum claimants as either witnesses or victims of smuggling to justify taking their devices and gathering of all their data.

45. We emphasise the above concerns, particularly acute where there are additional issues of language and other factors, whether asylum seekers, refugees and other migrants could ever 'voluntarily' hand over the devices and 'agree' to data. With the fear that a claim may be rejected if they do not hand over their phones.

46. If the powers at Chapter 3 Part 2 are to remain in the Bill, the 'authorised persons' definition must be limited to police officers and constables.

Failure to provide for adequate oversight, notification and redress mechanisms

47. There is a marked absence in the PCSC Bill of detail of independent oversight, notification and redress mechanisms to safeguard individuals' privacy rights and ensure compliance with Article 8 ECHR. The UN General Assembly Resolution on the Right to Privacy in the Digital Age expressly called for establishment of independent and effective oversight mechanisms capable of ensuring transparency and accountability for

[24] UN, Human Rights Committee, Concluding Observations on the UK, July 2015 http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fGBR%2fCO%2f7&Lang=en

State surveillance of communications, their interception and collection of personal data.[25] Further, in *Szabó and Vissy v Hungary,* the ECtHR stated that redress mechanisms for any abuse sustained are important for reinforcing citizens' trust.[26] Additionally, the Report of the Office of the UN High Commissioner for Human Rights, provided that notice is one of the critical issues in determining access to an effective remedy.[27] The ECtHR also previously stated notification needs to be made to the persons concerned as soon as it can be made without jeopardising the purpose of surveillance.[28]

48. The PCSC Bill states in section 40 that the Code of Practice will be published, which will outline more details about how the powers can be practically used. We submit it would be unacceptable to leave such provisions to a Code of Practice. The Bill lacks statutory safeguards to protect against arbitrary interference and abuse, in violation of requirement of legality under international human rights law.

49. This is worrying in light of the above noted findings of the ICO report regarding security risks. The ICO's investigation also highlighted that there were numerous security concerns regarding unauthorised access and unintentional disclosure of extracted data. The highly sensitive personal data held was not always being encrypted whilst being exported to other digital media. The unencrypted data was variously put on CDs, DVDs and USB drives, and often transported by couriers or other unsecured means.[29]

50. Thank you for your consideration of these comments. We are content to have this submission published and attributed to our organisations.

[25] UN General Assembly Resolution on the Right to Privacy in the Digital Age U.N. Doc. A/RES/73/179 (17 December 2018) para 6.
[26] *Szabó and Vissy v. Hungary*, (No. 37138/14, 12 January 2016) para 79
[27] Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (30 June 2014) para 40
[28] Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (30 June 2014) para 40
[29] ICO, Investigation Report: Mobile Phone Data Extraction by Police Forces in England and Wales (June 2020) p. 48, available at: https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf

Annex 1: What is needed to inform an individual (non-exhaustive list)

Extraction:

- What data has been extracted
- Whether it is possible to selectively extract certain types of data
- If yes, whether authorities will restrict the extractions to certain types of data
- If no, and they have to extract all data, what limits exist in relation to the examination of the data i.e. how is the police officer who is viewing the data restricted to looking only at what is strictly necessary and proportionate
- Whether it is possible to selectively extract data by type and time frame i.e. extract only messages relating to a certain period
- If yes, whether they will restrict the extraction to this
- If no, and they have to extract all data, what limits exist in relation to the examination of data i.e. how is the police officer who is viewing the data restricted to looking only at what is strictly necessary and proportionate
- Whether cloud extraction is used for electronic devices

Examination:

- What data will and has been examined e.g. provision of a list of data types, dates etc
- How the authorised person will decide which data to examine;
- What independent checks exist to ensure that the authorised person only examines what is strictly necessary;
- What auditing exists to ensure that authorised persons only examine what is strictly necessary and reasonable in relation to the investigation;
- Is all extracted and examined data retained;
- On what basis is irrelevant data retained and not deleted;

Disclosure:

- What data will the authorised person disclose to an individual who is not the user of the device e.g. disclosing data obtained from a victim to a suspect
- What details will be provided to an individual who is the user of the device in relation to a detailed description of the data provided to another individual i.e. a victim's data provided to a suspect.