NORTHERN IRELAND HUMAN RIGHTS COMMISSION

Submission to the Committee for Justice on Provisions from the Police, Crime, Sentencing and Courts Bill that apply to Northern Ireland.

April 2021

Table of Contents

Recommendations

2.18 The NIHRC advises that amendments to section 3 of the COPO Act concerning communications data (or metadata) impact on the rights to privacy and freedom of expression. Further safeguards are required to ensure that the acquisition of metadata does not violate Articles 8 and 10 of the ECHR.

2.21 The NIHRC recommends that further information is sought on who will be a "prescribed person" in advance of an LCM and to ensure that effective oversight mechanisms are in place to cover such individuals.

2.22 The NIHRC recommends that the additional judicial oversight provision outlined in Schedule 5, paragraph 3 should be monitored to ensure it is being implemented effectively.

3.15 The NIHRC advises that the Committee for Justice may wish to request additional information from the Home Office regarding how individuals subject to SHPOs or SROs who move between jurisdictions will be identified within the new jurisdiction to ensure that effective monitoring is achieved.

4.5 The NIHRC welcomes statutory provisions for training courses as an alternative to fixed penalties for low-level driving offences. The NIHRC recommends that any increase to fees for these courses is not prohibitive to ensure equal access for all.

4.6 The NIHRC recommends that any change in policy relating to the cost of course alternatives to fixed penalties is accompanied by at Section 75 equality impact assessment to ensure that it is not impacting on equality of opportunity alongside notification to the Committee of any increase against the actual administrative costs incurred.

5.12 The NIHRC advises that the Committee may wish to consult with the Independent Commission for the Location of Victims' Remains to garner their views in respect to any potential implications of Schedule 6 on their ongoing work.

1 Introduction

1.1 The Northern Ireland Human Rights Commission (NIHRC), pursuant to section 69(1) of the Northern Ireland Act 1998, reviews the adequacy and effectiveness of law and practice relating to the protection of human rights in Northern Ireland (NI). In accordance with this function, the following advice is submitted in response to Committee for Justice's (the Committee) request for the NIHRC's views on provisions within the Police, Crime, Sentencing and Courts Bill (PCSC) that will apply to Northern Ireland if a Legislative Consent Motion is approved.

1.2 The NIHRC bases its advice on the full range of internationally accepted human rights standards, including the European Convention on Human Rights, as incorporated by the Human Rights Act 1998, and the treaty obligations of the Council of Europe (CoE) and United Nations (UN). The relevant regional and international treaties in this context include:

- European Convention on Human Rights 1950 (ECHR);[1]
- UN International Covenant on Civil and Political Rights 1966 (UN ICCPR);[2]
- UN Convention on the Elimination of Discrimination against Women 1979 (UN CEDAW);[3]
- UN Convention against Torture 1984 (UN CAT);[4]
- UN Convention on the Rights of the Child 1989 (UN CRC);[5]
- UN Convention on the Rights of Persons with Disabilities 2006 (UN CRPD).[6]
- Council of Europe Convention No. 210 on Preventing and Combatting Violence against Women and Domestic Violence.[7]

1.3 In addition to these treaty standards, there exists a body of 'soft law' developed by the human rights bodies of the CoE and UN. These declarations and principles are non-binding but provide further guidance in respect of specific areas.

1.4 The NIHRC welcomes the opportunity from the Committee for Justice to respond to the specific provisions within the PCSC Bill. This response is

---

[1] Ratified by the UK in 1951.
[2] Ratified by the UK in 1976.
[3] Ratified by the UK in 1986.
[4] Ratified by the UK in 1988.
[5] Ratified by the UK in 1991.
[6] Ratified by the UK in 2009.
[7] Signed by the UK in 2012.

structured around the five provisions specified by the Committee. This includes: (i) amendments to the Crime (Overseas Production Orders) Act 2019; (ii) cross-jurisdictional enforcement of Scottish Sexual Harm Prevention Orders and Sexual Risk Orders; (iii) a statutory authority for charging for courses as an alternative to fixed driving penalties; (iv) police powers to access information relating to the location of human remains; and (v) powers to extract information from mobile devices.

2 Overseas Production Orders

Background

2.1 The Crime (Overseas Production Orders) Act 2019 (COPO Act) enables appropriate officials to make an application for stored electronic information held outside of the UK for use in the investigation and prosecution of serious crimes.[8] Prior to the COPO Act, UK authorities could seek access to data from overseas using Mutual Legal Assistance Treaties (MLATs)[9]; however, these are considered by the government to be overly bureaucratic and time consuming for officials involved in security and law enforcement.[10] The COPO Act was enacted to grant law enforcement and prosecution agencies the power to obtain Overseas Production Orders (OPOs) in UK courts against persons in other jurisdictions providing there is a relevant international co-operation agreement in place.[11]

2.2 Section 1 COPO Act permits a judge to make an overseas production order in respect of electronic data if a number of conditions are fulfilled. These conditions are listed under Section 4 COPO Act and require a judge to be satisfied that:

- that the person against whom the order is sought operates or is based in a country outside the UK which is party to an international co-operation agreement[12];
- there are reasonable grounds for believing an indictable offence has been committed and that proceedings for this offence have commenced or it is already being investigated or the order is sought for the purposes of investigating terrorism[13];
- the person possesses all or part of the data being sought[14];

---

[8] The Home Office, 'Crime (Overseas Production Orders) Bill: Explanatory Notes', 27 June 2018, at 2.
[9] House of Lords, 'Crime (Overseas Production Orders) Bill', HL Bill 113 of 2017-19, at 3.
[10] Ibid, at 4
[11] House of Commons Library, 'Police, Crime, Sentencing and Courts Bill: Part 2, Prevention, investigation and prosecution of crime', 2021, at 40. Currently the only agreement in place is the UK-US Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime, which came into force in 2020.
[12] Section 4(2)
[13] Section 4(3)
[14] Section 4(4)

- there are reasonable grounds to believe that some or all of the data being sought will be of substantial value to the investigation or proceedings, and it is in the public interest that this data is made available to the investigation or proceedings.[15]

2.3 In 2019, eight NGOs signed a letter arguing that aspects of the then COPO Bill were not compliant with international human rights standards. They argued that the Bill would contravene the right to privacy and the right to freedom of expression.[16] The NGOs addressed issues concerning the disparity between the minimum threshold for an order in the COPO Bill and the Investigatory Powers Act 2016[17] and the need for robust checks and safeguards within the Bill to address protections on applications from other States for access to data held in the UK.[18] These issues have not been addressed within the COPO Act or in the proposed amendments within the COPO Bill.

Overseas Production Orders and Human Rights Compliance

2.4 The right to respect for private and family life is protected by Article 8 ECHR and Article 17 ICCPR. Similar provisions are also contained within the UNCRPD[19] and the UNCRC.7[20]

2.5 The engagement of Article 8 ECHR has been confirmed by the European Court of Human Rights (ECt.HR), in its conclusion that the storage of information relating to an individual's private life in an interference with Article 8.[21] The subsequent use of that stored data does not affect this finding.[22] Article 8(2) identifies the right to privacy as a qualified right, requiring that any limitation must be exercised "in accordance with the law" and be "necessary in a democratic society". The ECt.HR has afforded states a wider margin of appreciation in relation to Article 8 and as a result, States have a level of discretion in how they choose to limit this right.[23] Determining whether an interference with the right to privacy is

---

[15] Section 4(5)-(7)
[16] CAGE, 'Why Cage Believes the New Crime (Overseas Production Orders) Bill should alarm all who care about privacy', accessed at Why CAGE believes the new Crime (Overseas Production Orders) Bill should alarm all who care about privacy. - CAGE
[17] Ibid; the Investigatory Powers Act states a warrant can only be deemed necessary if it is in the interests of national security, the prevention or detection of serious crime, or in the interests of the economic well-being of the UK so far is relates to national security. The COPO Act requires that there be reasonable grounds to believe an indictable offence has been committed, unless the order is sought in respect of a terrorist investigation, where no evidential threshold is required.
[18] Ibid.
[19] Article 22 UNCRPD.
[20] Article 16 UNCRC.
[21] Leander v Sweden (1987) 9 EHRR 433.
[22] Amann v Switzerland (2000) ECHR 88.
[23] S and Marper v The United Kingdom (2008) ECHR 1581, at para 66.

justified is guided by whether it is "proportionate to the legitimate aim pursued".[24]

2.6 Article 17 ICCPR similarly protects against "arbitrary interference" of a person's privacy. The UN Human Rights Committee (UN HRC) identifies, in its General Comment No 16 on Article 17, that arbitrary interference can extend to interference provided for under the law.[25]

2.7 The (then) Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (Terrorism), Martin Scheinin, has called upon States to justify why any limitation to Article 17 is legitimate.[26] Furthermore, in its consideration of violations to Article 17, the UN HRC has applied the requirements of legitimate aim, necessity and proportionality.[27]

2.8 The UK is internationally obligated to respect, protect and fulfil the human rights of those under its jurisdiction. These obligations include putting in place robust legal frameworks to ensure individual rights are protected. The State is bound by positive obligations to protect the right to life under Article 2 ECHR and the prohibition of torture, inhumane and degrading treatment under Article 3 ECHR.[28] Requirements under these rights include an investigative obligation. Under Articles 2 and 3 ECHR an investigation should be independent, capable of identifying those responsible, be prompt, have a degree of public scrutiny and have involvement from the victim or next of kin.[29]

2.9 Section 4(3)(a) of the COPO Act identifies that an OPO can be sought if a judge is satisfied that there are reasonable grounds to believe that an indictable offence has been committed. Section 4(3)(b) allows for an OPO if a judge is satisfied that the order is being sought for the purposes of a terrorist investigation. Meeting the evidential threshold is not required when applying for electronic data in relation to terrorism investigations. Digital privacy NGOs have identified that this provision violates due

---

[24] *Dudgeon v United Kingdom* (1981) ECHR 5, at para 53.
[25] UN Human Rights Committee, CCPR General Comment No 16: Article 17 The right to respect of privacy, family, home and correspondence, and protection of honour and reputation, 8 April 1988. See para 4; the introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances.
[26] A/HRC/13/37, Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism' Thirteen Session, 28 December 2009, at para 18.
[27] Van Hulst v. The Netherlands, communication No. 903/1999, 2004.
[28] See also Articles 6 and 7 ICCPR; UNCAT.
[29] Jordan v. the United Kingdom, Application No. 24746/96 (4 August 2001) paras 106-9.

process rights.[30] The (then) Special Rapporteur on Terrorism has also identified that surveillance measures can violate due process rights when individuals are unable to prove that they are actually under surveillance.[31]

2.10 The Special Rapporteur on the right to privacy has identified that, where some UN Member States may have domestic legislation governing surveillance practices in relation to the right to privacy, it is "largely silent on what happens when personal data is shared across borders and what further safeguards should be put in place in such cases".[32] The Special Rapporteur cites the Snowden revelations as being a catalyst for both States to legislate on surveillance and privacy.[33] These legislative changes have involved constraints and safeguards and on other occasions have legitimised practices.[34]

2.11 Article 10 ECHR protects the right to freedom of expression.[35] Article 10 protects the "freedom to hold opinions and to receive and impart information and ideas without interference from public authorities". Article 10(2) identifies that there can be limitations to the right to freedom of expression if they are prescribed by law and are necessary in a democratic society.

2.12 ECt.HR jurisprudence on Article 10 ECHR protects journalistic freedom, including by finding violations to Article 10 where a State has interfered with a journalist's research or investigatory activities. In the Sunday Times v the United Kingdom, the ECt.HR held there had been a violation of Article 10. The Sunday Times attempts to publish details of a memoir by a former member of the British Security Services, who alleged that the Service had engaged in illegal conduct, were impeded by various injunctions obtained by the British Government, who argued that the memoir contained confidential information.[36] The Government argued that curtailing Article 10 in this circumstance was "necessary in a democratic society".[37] The ECt.HR did not regard the Government's argument as sufficient to justify an interference with Article 10, noting that they prevented newspapers

---

[30] CAGE, 'Why Cage Believes the New Crime (Overseas Production Orders) Bill should alarm all who care about privacy', accessed at Why CAGE believes the new Crime (Overseas Production Orders) Bill should alarm all who care about privacy. - CAGE
[31] UN Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, A/HRC/13/3 (28 December 2009), at para 38.
[32] UN Human Rights Council, Report of the Special Rapporteur on the Right to Privacy, A_HRC_37_62_EN (28 February 2018), at para 27.
[33] Ibid, at footnote 46. The Snowden revelations exposed mass surveillance and other privacy-intrusive programmes carried out by the UK and USA intelligence communities.
[34] Ibid.
[35] See also; Article 19 ICCPR, Article 21 UNCRPD and Article 13 UNCRC.
[36] Ibid
[37] Ibid, at para 50; See also para53, the Government identified that their restraints on the Sunday Times were necessary to protect national security and prevent the publishing of an unauthorised memoir containing confidential material.

from "exercising their right and duty to purvey information, already available, as a matter of legitimate public concern".[38]

2.13 In the case of Big Brother Watch and Others v the United Kingdom, the ECt.HR heard how the acquisition of bulk data or "metadata" by UK intelligence authorities could have positive impacts for investigators as they would be able to look for unknown dangers as opposed to only being able to investigate known dangers. However, the ECt.HR heard from a Report by the European Commission for Democracy through Law that the requirement for telecommunications companies to store and then provide this data amounted to an interference to the right to privacy.[39] The acquisition of metadata can provide so much information that the content of the original data is not necessary.[40] This is particularly pertinent to journalists who have to protect their sources, yet the acquisition of related metadata could by itself reveal the identification of informants.[41] The Court noted that safeguards exist in relation to the storing of confidential material once identified, but identified the "potential chilling effect that any perceived interference with the confidentiality of their communications and, in particular, their sources might have on the freedom of the press".[42] As a result, there had been a violation to Article 10 in relation to press freedom.[43]

2.14 Section 12 of the COPO Act identifies that OPOs can be used to intercept data containing journalistic material. When the then COPO Bill was introduced in Parliament, several privacy rights NGOs outlined their concerns that this legislation would impact on journalists' ability to conduct work in the public interest.[44]

Amendments to the COPO Act in the Police, Crime, Sentencing and Courts Bill

2.15 Work on implementing OPOs has identified certain issues that the PCSC Bill intends to address through amendments to the COPO Act 2019 through clause 47, which introduces Schedule 5.

---

[38] Ibid, at paras 55-56.
[39] Big Brother Watch and Others v the United Kingdom [2018], at para 211.
[40] Ibid, at para 301.
[41] Ibid, at para 484.
[42] Ibid, at para 495.
[43] Ibid, at 495.
[44] CAGE, 'Why Cage Believes the New Crime (Overseas Production Orders) Bill should alarm all who care about privacy', accessed at Why CAGE believes the new Crime (Overseas Production Orders) Bill should alarm all who care about privacy. - CAGE

2.16 Section 3 of the COPO Act identifies that communications data is excepted from applications for OPOs. Communications data is metadata,[45] referring to the "who, where, when and how of a communication but not its content".[46] Paragraph 2 of Schedule 5 of the Bill amends Section 3 of the COPO Act to provide that metadata that is "comprised in, included as part of, attached to or logically associated with" electronic data can be included in an application for an OPO. In a briefing paper regarding this provision within the Bill, it is noted that this data is necessary to provide the electronic content data with the necessary content to be treated as evidence.[47] As noted above, the acquisition of metadata has implications on Article 8 ECHR on the right to privacy, and has specific connotations for Article 10 ECHR on freedom of expression in relation to journalistic material, as metadata can identify journalists' sources.

2.17 Section 8 of the COPO Act applies to the inclusion of non-disclosure requirements in OPOs. In a briefing paper on the PCSC Bill, Fair Trials noted that the circumstances in which non-disclosure requirements can be made are not clear, meaning persons who are subject to an OPO may not be made aware that there is an order against them.[48] Fair Trials further identifies that the COPO Act contains insufficient safeguards for persons against whom the order is sought and the amendments within the PCSC Bill do not effectively address this issue.[49]

2.18 **The NIHRC advises that amendments to section 3 of the COPO Act concerning communications data (or metadata) impact on the rights to privacy and freedom of expression. Further safeguards are required to ensure that the acquisition of metadata does not violate Articles 8 and 10 of the ECHR.**

2.19 Section 5 of the COPO Act currently provides that, when making a decision on an OPO in respect to data, a judge must be satisfied that all or part of the data is likely to be of substantial value and that it is in the public interest that all or part of the data is produced. Schedule 5, paragraph 3 of the PCSC Bill seeks to amend this to include that a judge must also be satisfied that there are reasonable grounds to believe that all or part of the data is likely to be relevant evidence.[50] The NIHRC recognises that this

---

[45] Big Brother Watch, 'Why Communications Data (Metadata) Matter', accessed at Communications-Data-Briefing.pdf (bigbrotherwatch.org.uk)
[46] Home Office, 'Communications Data' (2015), accessed at Communications data - GOV.UK (www.gov.uk)
[47] House of Commons Library, 'Police, Crime, Sentencing and Courts Bill 2019-21: Part 2- Prevention, Investigation and Prosecution of Crime', (2021).
[48] Fair Trials, 'Police, Crime, Sentencing and Courts Bill: Fair Trials Briefing for Second Reading', (2021), at 11, accessed at Fair Trials Police Crime Sentencing and Courts Bill briefing for Second Reading.pdf
[49] Ibid.
[50] House of Commons Library, 'Police, Crime, Sentencing and Courts Bill 2019-21: Part 2- Prevention, Investigation and Prosecution of Crime', (2021), at 41.

extended judicial oversight is an additional safeguard to the process for applying for an OPO within the PCSC Bill. Fair Trials have identified that the amendments within the PCSC Act do not effectively address issues around safeguards for defendants, as non-disclosure orders may still be made against those to which OPOs apply.[51] The NIHRC would suggest that the implementation of this additional judicial oversight be monitored closely to ensure it is being applied as an effective and adequate safeguard.

2.20 Schedule 5 amends Sections 9 and 14 of the COPO Act to allow a "prescribed person" to serve OPOs. Currently the Act only provides that the Secretary of State can serve OPOs made in England, Wales and Northern Ireland and the Lord Advocate can serve OPOs made in Scotland. The amendment seeks to extend the restrictions on service of an order to a prescribed person, which refers to a person prescribed by regulations made by the Secretary of State or the Lord Advocate.[52] Regulations relating to these prescribed persons have not been released, nor is there guidance regarding what constitutes appropriate infrastructure. Additionally, questions arise over whether these prescribed persons will be subject to the same oversight provisions as the Secretary of State and the Lord Advocate.

2.21 **The NIHRC recommends that further information is sought on who will be a "prescribed person" in advance of an LCM and to ensure that effective oversight mechanisms are in place to cover such individuals.**

2.22 **The NIHRC recommends that the additional judicial oversight provision outlined in Schedule 5, paragraph 3 should be monitored to ensure it is being implemented effectively.**

3 Cross-Jurisdictional Enforcement of Scottish Sexual Harm Prevention Orders and Sexual Risk Orders

Human Rights Standards in relation to Sexual Offences

3.1 Serious sexual offences engage a number of human rights standards, including Article 3 ECHR on the prohibition of torture and cruel, inhumane or degrading treatment.[53] Article 3 ECHR is an absolute right, which

---

[51] Fair Trials, 'Police, Crime, Sentencing and Courts Bill: Fair Trials Briefing for Second Reading', (2021), at 11, accessed at Fair Trials Police Crime Sentencing and Courts Bill briefing for Second Reading.pdf
[52] House of Commons Library, 'Police, Crime, Sentencing and Courts Bill 2019-21: Part 2- Prevention, Investigation and Prosecution of Crime', (2021), at 41; The rationale behind this amendment is to ensure that this function can be securely discharged by a body with the appropriate infrastructure to securely receive and transmit data from service providers based overseas.
[53] See also; Article 7 ICCPR and UNCAT.

provides that this right cannot be interfered with under any circumstances.[54] The right to private and family life may also engaged in cases of serious sexual offences, under Article 8 ECHR, in particular where the threshold for Article 3 ECHR is not met.[55]

3.2 While international human rights standards generally apply to the State, there has been recognition of the application of human rights protections where harm is caused by non-state actors. The ECt.HR has held that States Parties have a responsibility to protect individuals against violence by third parties. This has been particularly evident in relation to violations under Articles 2 and 3 ECHR, but Article 8 has also been applied given that violence threatens the bodily integrity aspect of the right to private life.[56]

3.3 The UN Committee against Torture (CAT) identified, through General Comment No 2, that a State's indifference or inaction to non-State actors committal of impermissible acts under the Convention amounts to "de facto permission".[57] The Committee has applied this principle to to States parties' "failure to prevent and protect victims from gender-based violence, such as rape, domestic violence, female genital mutilation, and trafficking".[58]

3.4 Sexual violence is internationally recognised as a form of gender-based violence against women and constitutes discrimination against women.[59] Article 2 UN CEDAW obliges States Parties to "adopt appropriate legislative and other measures… prohibiting discrimination against women". This is an immediate obligation comprising two aspects of state responsibility including for violence resulting from the actions or omissions of the State Party, and non-state actors.[60]

3.5 The Istanbul Convention creates obligations on the State in respect of sexual violence. Article 36 obliges States Parties to take all legislative and other measures to ensure that sexual violence is criminalised. Article 45 of the Convention obligates States to ensure that sexual offences are punishable by effective, proportionate and dissuasive sanctions, including monitoring and supervision of convicted persons.

---

[54] Chahal v UK (1996) ECHR 413.
[55] See also Article 17 ICCPR.
[56] Milićević v Montenegro (2018) ECHR 6; ES. and Others v. Slovakia (2009).
[57] UN Committee against Torture, General Comment 2: Implementation of article 2 by States parties, CAT/C/GC/2 (24 January 2008) para 18.
[58] Ibid.
[59] Article 1 CEDAW.
[60] UN Committee on the Elimination of Discrimination against Women, General Recommendation 35: gender-based violence against women, updating general recommendation No. 19, CEDAW/C/GC/35 (14 July 2017), at para 21.

3.6 Article 19 of the UNCRC requires States to "take all appropriate legislative… measures to protect the child from all forms of physical or mental violence… including sexual abuse". The Committee on the Rights of the Child has identified that legislative measures refers to both legislation, including a budget and implementation and enforcement procedures.[61]

Background

3.7 The Scottish Government legislated for new preventative orders in relation to sexual offenders or those whose behaviour indicates risk of sexual harm through the Abusive Behaviour and Sexual Harm (Scotland) Act 2016. The new orders, the Sexual Harm Prevention Order (SHPO) and the Sexual Risk Order (SRO), replaced existing orders in Scotland and are intended to mirror equivalent changes to preventative orders made in England and Wales.

3.8 The PCSC Bill proposes to amend the Sexual Offences Act 2003 to give these orders cross-jurisdictional enforcement across the UK. Without cross-jurisdictional enforcement the orders will not be enforceable outside of Scotland meaning persons subject to these orders could move to another UK jurisdiction to evade an order, a breach of an order outside of Scotland will not constitute a criminal offence and notification requirements regarding these orders would only apply in Scotland.[62]

Provisions within the Police, Crime, Sentencing and Courts Bill that are applicable to Northern Ireland in relation to SHPOs and SROs

3.9 Clause 150 of the PCSC Bill proposes to amend section 351 of the Sentencing Code and Section 113 of the Sexual Offences Act 2003 to account for a breach of a positive requirement under a SHPO or SRO in NI. Positive requirements are outlined in Clause 148 of the PCSC Bill, which identifies that these are positive obligations to allow courts to require individuals subject to SHPOs and SROs to engage in specified activities. These could include behavioural change programmes, alcohol or drug treatments or to attend polygraph tests.[63]

3.10 Additionally, Clause 150 amends Section 136ZA of the Sexual Offences Act 2003 to ensure that positive requirements under the new orders will apply throughout the UK. Clause 150 also amends Sections 136ZC and 136ZD of the Sexual Offences Act 2003 to allow for courts in NI to vary positive requirements of SHPOs and SROs.

---

[61] UN Committee on the Rights of the Child, General Comment No 13: The right of the child to freedom from all forms of violence, CRC/C/GC/13 (18 April 2011).
[62] Information provided by the Department of Justice, 8 January 2021.
[63] Home Office, 'Police, Crime, Sentencing and Courts Bill: Explanatory Notes' (2021), at para 1101.

3.11 Clause 153 of the PCSC Bill proposes to amend Sections 103I, 113, 122, 122H and 128 of the Sexual Offences Act to allow the orders created in Scotland under the Abusive Behaviour and Sexual Harm (Scotland) Act to be enforceable in England, Wales and Northern Ireland. Clause 153 will also amend Section 136ZA of the Sexual Offences Act 2003 to allow SHPOs and SROs to apply throughout the UK.

3.12 Clause 155 of the PCSC Bill proposes to amend Section 136ZB of the Sexual Offences Act 2003 to clarify orders superseding or superseded by Scottish SHPOs and SROs. Clause 155(4) of the PCSC Bill amends Section 126ZB(2) to clarify that when a new Sexual Offences Prevention Order (SOPO), Foreign Travel Order (FTO) or Risk of Sexual Harm Order (RSHO) is made in NI, earlier orders, whether issued by courts in England, Wales or Scotland cease to have effect.

3.13 Clause 156 of the PCSC Bill introduces Schedule 17, which contains proposed amendments to the Sexual Offences Act 2003 enabling a court in one part of the UK to vary, renew or discharge an order made in another part of the UK. Clause 156(2) of the Bill further explains Schedule 17, stating that:

- Part 1 enables a court in Northern Ireland to renew or discharge orders made in England and Wales and to vary, renew or discharge orders made in Scotland;
- Part 2 enables a court in Scotland to vary, renew or discharge orders made in England and Wales or Northern Ireland; and
- Part 3 enables a court in England and Wales to vary, renew or discharge orders made in Scotland or Northern Ireland.

3.14 Neither the Clauses within the Bill relating to provisions around SHPOs or SROs or Schedule 17 identify how the government plans to monitor the movement of offenders from one jurisdiction to another. It would be helpful to address the practical application of these orders as well as ensuring their operational function to ensure that they are as effective as possible. It is also important that how offenders' movement between jurisdictions is monitored is compliant with international human rights standards.

3.15 **The NIHRC advises that the Committee for Justice may wish to request additional information from the Home Office regarding how individuals subject to SHPOs or SROs who move between jurisdictions will be identified within the new jurisdiction to ensure that effective monitoring is achieved.**

4 National Driver Offender Retraining Scheme

4.1 Clause 67 of the PCSC Bill would provide for statutory provisions for a charging regime for courses offered as an alternative to prosecution in England, Wales and Scotland. Clause 67(2) seeks to amend the Road Traffic Offenders (Northern Ireland) Order 1996 to extend these powers to NI.

4.2 The powers that Clause 67(2) intends to extend include conferring powers for the Chief Constable to charge a fee for alternative courses, with approval from the Policing Board at a level that exceeds the cost of the course and related administrative expenses. Subsection (2) identifies that any excess funds raised through these charges must be used for the purpose of promoting road safety. Subsection (4) identifies that the Department of Justice (DoJ) can, by regulations, make further provisions about how fees are to be calculated, the level or fees and the use of fee income.

4.3 Article 14 ICCPR protects equal access to the administration of justice.[64] The ability to raise additional funds to promote road safety is welcome. However, the Commission would note that new course fees should not be prohibitive so that fees will not disproportionately impact low income households, marginalised groups or those living in poverty, ensuring equal access to training courses as an alternative to a fixed penalty.

4.4 Section 75 of the Northern Ireland Act 1998 creates a statutory duty on public authorities to have due regard for the need to promote equality of opportunity between protected characteristics. Section 75 equality impact assessments identify policies that are likely to have a negative impact on equality of opportunity. The DoJ could ensure that any policy change regarding course fees is accompanied by an equality impact assessment to ensure that any rise in costs does not have a disproportionate impact on protected characteristics alongside a commitment to notify the Justice Committee of any increase against the actual administrative costs incurred..

4.5 **The NIHRC welcomes statutory provisions for training courses as an alternative to fixed penalties for low-level driving offences. The NIHRC recommends that any increase to fees for these courses is not prohibitive to ensure equal access for all.**

4.6 **The NIHRC recommends that any change in policy relating to the cost of course alternatives to fixed penalties is accompanied by at**

---

[64] See also; Article 6 ECHR, Article 15 UNCEDAW and Article 12 UNCRPD.

Section 75 equality impact assessment to ensure that it is not impacting on equality of opportunity alongside notification to the Committee of any increase against the actual administrative costs incurred.

5 Material Relating to the Location of Human Remains

Background

5.1 Section 8 of the Police and Crime Evidence Act 1984 (PACE) enables the police or a justice of the peace to obtain a warrant to enter and search a premises and seize evidence. The Home Office identified a gap in respect of s.8 through the case of Keith Bennett, a 12-year old boy who was abducted and killed by Ian Brady and Myra Hindley in the 1960s. After Brady's death in 2017, he left two briefcases that he had suggested contained information relating to the location of Keith's body in the possession of his solicitor. A magistrate denied an application for a warrant as they had determined that, since both Brady and Hindley had died, it was no longer possible to bring a prosecution in relation to Keith's death.[65]

Human Rights Standards in relation to the recovery of human remains.

5.1 While no international human rights instruments expressly refer to the rights and treatment of the dead, there are specific rights that are relevant in this area. The Declaration on the Protection of all Persons from Forced Disappearance[66] states in Article 1 that disappearance engages the right to life,[67] the right to recognition before the law,[68] the right to liberty and security of the person[69] and the right not to be subjected to torture and other cruel, inhuman or degrading treatment or punishment.[70]

5.2 The UK government's obligations under Article 2 ECHR (right to life) and Article 3 ECHR (prohibition of torture and other cruel, inhumane or degrading treatment or punishment) extends to conducting an official, effective investigation, which must be independent, capable of identifying those responsible, be prompt, and there must be public scrutiny with the

---

[65] Ibid.
[66] UN General Assembly, 'The Declaration on the Protection of all Persons from Enforced Displacement' Adopted by General Assembly Resolution 47/133 of 18 December 1992; Enforced disappearances are defined by the Working Group on Enforced or Involuntary Disappearances as having some level of governmental knowledge or involvement, and thus is not representative of the purposes of this legislation. However, these rights may also be engaged in cases of disappearances as a result of non-state actors.
[67] See Article 2 ECHR, Article 6 ICCPR, Article 10 UNCRPD and Article 6 UNCRC.
[68] See Article 12 ECHR, Article 16 ICCPR, Article 12 UNCRPD, Article 15 UNCEDAW and Article 5 UNCERD.
[69] See Article 5 ECHR, Article 9 ICCPR and Article 14 UNCRPD.
[70] See Article 3 ECHR, Article 7 ICCPR and UNCAT

participation of the next-of-kin.[71]. The ECt.HR has found violations of Article 2 in respect of State failure to conduct an effective investigation into clarifying the whereabouts of missing persons who disappeared in life threatening circumstances.[72] The ECt.HR has also found violations of Article 3 ECHR in respect of State failure to assist in the search for the truth about the whereabouts of a missing relative.[73]

5.3 The acquisition of an order to enable police to search a property or remove material without the consent of the relevant person to which the order applies engages Article 8 ECHR on the right to privacy. These new provisions may also engage Article 1 of Protocol 1 (A1P1) ECHR on the protection of property, which states "every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law".

5.4 In a letter to the Chair of the Joint Committee on Human Rights, the government recognised that Article 8 and A1P1 will be engaged by the new provisions in the PCSC Bill, but identified that judicial safeguards built into the new powers should ensure that they are used only as a last resort.[74]

5.5 The new provisions within the PCSC Bill may also engage article 10 ECHR on the right to freedom of expression where orders pertain to material that includes journalistic material. Article 10(1) ECHR states that everyone has the right to freedom of expression. Article 10(2) ECHR identifies that any interference with freedom of expression must be "prescribed by law" and "necessary in a democratic society".

<u>Provisions within the Police, Crime, Sentencing and Courts Bill on the recovery of human remains relating to Northern Ireland</u>

5.6 Clause 51(1) of the PCSC Bill introduces Schedule 6, which allows authorities to apply to access excluded material or special procedure material that relates to the location of human remains provided specific conditions are met.[75]

---

[71] Hugh Jordan v. the United Kingdom, at paras 105 – 109.
[72] Cyprus v. Turkey, Application No. 25781/94, 10 May 2001, para 136.
[73] Kurt v. Turkey, Application No. 15/1997/799/1002, 25 May 1998, para 175..
[74]Home Office and Ministry of Justice, Letter to Rt Hon Harriet Harman, Chair Joint Committee on Human Rights on Police, Crime, Sentencing and Courts Bill, 9 March 2021.
[75] Clause 50 of the PCSC Bill identifies that excluded material and special procedural material have the same meaning as in Sections 11 and 14 of the Police and Criminal Evidence Act 1984 (PACE) respectively. Section 11 of the PACE Act identifies that excluded material includes personal records acquired in the course of any trade, business, profession or other occupation, human tissue or tissue fluid taken for the purpose of medical treatment and journalistic material which a person holds in confidence. Section 14 of the PACE Act defines special procedural material as journalistic material other

5.7 Clause 51(2) identifies that, under Section 29 of the Petty Sessions (Ireland) Act 1851, warrants granted under Schedule 6 can be executed in Northern Ireland. The draft Bill's Explanatory Notes explain further:

> This provision therefore replicates insofar as possible section 9(2A) of the PACE. In effect, this ensures that a 'process' (a warrant or order) issued by a court in England or Wales under these powers and endorsed by a court in Scotland may be executed in Scotland (and vice versa). Section 29 of the 1851 Act provides equivalent provisions for execution in Northern Ireland.[76]

5.8 Paragraph 1 of Schedule 6 allows a judge to issue a warrant if the following conditions are met:

- There are reasonable grounds to believe that material that consists of, or may relate to the location of, relevant human remains is in the possession or control of the person specified in the application, or is in the premises occupied or controlled by the person specified in the application.
- There are reasonable grounds to believe the material consists of or includes excluded material or special procedural material.
- There are reasonable grounds to believe that the material does not consist of or include items subject to legal privilege.
- Other methods to obtain the material have been tried without success or have not been tried because it appeared they were bound to fail.
- It must be in the public interest, having regard to the need to ensure that human remains are located and disposed of in a lawful manner and to the circumstances under which the person in possession of the material came to hold it.

5.9 Paragraph 5(1) of Schedule 6 states that applications made in respect of material that is reasonably believed to consist of or include journalistic material must be made inter partes.[77]

5.10 While this legislation intends to allow police to obtain evidence in relation to the location of human remains where there is no longer an opportunity

---

than excluded material and material other than items subject to legal privilege and excluded material, which was acquired in the course of any trade, business, profession or other occupation or for the purpose of any paid or unpaid office that they hold in confidence.

[76] Home Office, 'Police, Crime, Sentencing and Courts Bill: Explanatory Notes' (2021), at para 484.

[77] Police, Crime, Sentencing and Crime Bill, Schedule 6, at para 5(1). Other provisions within Schedule 6 include; para 3 specifies that orders made in respect of stored electronic data must be produced in a form that can be taken away; para 2 states that any material specified in an order must be produced to a constable within 7 days from the date of the order, unless a longer period is specified on the order; and para 6(1) notes that once a warrant has been issued, a person may not hide, destroy, dispose or alter evidence.

to secure a conviction, there are specific issues in relation to the Bill's impact in Northern Ireland. As a result of the history of Northern Ireland, the bodies of many victims of the conflict have never been recovered. In response to this, the British and Irish governments established the Independent Commission for the Location of Victims' Remains (ICLVR) via an intergovernmental agreement signed on 27 April 1999.[78] In response to this agreement, both governments introduced legislation outlining the ICLVR's remit and powers. Section 3 of the UK legislation, the Northern Ireland (Location of Victims' Remains) Act 1999, identifies that 'any relevant information provided to the Commission and any evidence obtained (directly or indirectly) as a result of such information being so provided' shall not be admissible in evidence in any criminal proceedings.

5.11 Schedule 6 applies to warrants issued by courts in England and Wales but has cross-border application in Scotland and Northern Ireland. Where a warrant has effect in Northern Ireland it would be advisable to consult with the ICLVR, if there is a possibility of an overlap in jurisdiction.

5.12 **The NIHRC advises that the Committee may wish to consult with the Independent Commission for the Location of Victims' Remains to garner their views in respect to any potential implications of Schedule 6 on their ongoing work.**

6 Powers to Extract Information from Mobile Devices

6.1 Following concerns that police forces were inconsistent in their approach to extracting data from electronic devices for the purpose of investigating or prosecuting crimes, the Information Commissioner conducted an investigation into the practice of extracting electronic data.[79] The Information Commissioner identified the need for "better rules, ideally set out in a statutory code of practice, that will provide greater clarity and foreseeability about when, why and how the police and other law enforcement agencies use mobile phone data extraction (MPE)".[80]

6.2 The UK government intends to implement this recommendation through the PCSC Bill. The Department of Justice (DoJ) has previously sought the views of the NIHRC on the human rights compliance of provisions

---

[78] Independent Commission for the Location of Victims Remains, accessed at Home Page - The Department of Justice and Equality: (iclvr.ie)
[79] Information Commissioner's Office, 'Mobile Phone Data Extraction by Police Forces in England and Wales: Investigation Report' (ICO, 2020), at 7.
[80] Ibid, at 9.

contained within the PCSC Bill concerning the extraction of data from electronic devices. The Commission submitted a full response to the DoJ with recommendations in March 2021.[81] A copy of the Commission's response to the DoJ will be sent to the Committee alongside this submission.

Contact us

www.nihrc.org | info@nihrc.org | +44 (0)28 9024 3987

4th Floor, Alfred House, 19-21 Alfred Street, Belfast, BT2 8ED

[81] NI Human Rights Commission, 'Submission to the Department of Justice on Data Extraction from Electronic Devices', (NIHRC, 2021).

NORTHERN IRELAND HUMAN RIGHTS COMMISSION

Submission to the Department of Justice on Data Extraction from Electronic Devices

March 2021

Table of Contents

Recommendations

3.12 The NIHRC advises that the proposed Code of Practice should be published and consulted on in advance of the LCM to ensure its compliance with human rights standards. Subject to review of the code of practice, the NIHRC advises that an LCM would be appropriate to bring this chapter of the Police, Crime, Sentencing and Crime to the NI Assembly.

3.13 The NIHRC recommends that any individual or organisation listed as an "authorised person" in Schedule 3 of the Bill with jurisdiction in NI should be subject to specific oversight and required to publish the extent of the use of the powers and their circumstances.

4.3 The NIHRC recommends that any statutory code of practice in relation to data extraction from electronic devices which is applicable to NI should be produced in consultation with individuals and relevant organisations in NI.

4.6 The NIHRC recommends the proposed statutory code of practice should provide sufficient detailed guidance to enable those making decisions on the extraction of data from electronic devices to do so in an ECHR compliant manner.

5.7 The NIHRC advises that the Code of Practice should expressly address the unique impact data extraction has had on sexual assault cases and the legal guidance from *R v Bater-James* should be incorporated into the code to ensure legal certainty.

1.0 Introduction

1.1 The Northern Ireland Human Rights Commission (NIHRC), pursuant to section 69(1) of the Northern Ireland Act 1998, reviews the adequacy and effectiveness of law and practice relating to the protection of human rights in Northern Ireland (NI). In accordance with this function, the following advice is submitted in response to Department of Justice's request for the NIHRC's views on Chapter 3 of the Police, Crime, Sentencing and Courts Bill on data extraction from electronic devices.

1.2 The NIHRC bases its advice on the full range of internationally accepted human rights standards, including the European Convention on Human Rights, as incorporated by the Human Rights Act 1998, and the treaty obligations of the Council of Europe (CoE) and United Nations (UN). The relevant regional and international treaties in this context include:

- European Convention on Human Rights 1950 (ECHR);[1]
- UN International Covenant on Civil and Political Rights 1966 (UN ICCPR);[2]
- UN Convention on the Rights of the Child 1989 (UN CRC);[3]
- UN Convention on the Rights of Persons with Disabilities 2006 (UN CRPD).[4]
- Council of Europe Convention No. 108 on the Protection of Individuals with Regard to the Automatic Processing of Personal Data.[5]

1.3 In addition to these treaty standards, there exists a body of 'soft law' developed by the human rights bodies of the CoE and UN. These declarations and principles are non-binding but provide further guidance in respect of specific areas. These relevant standards in this context include:

- UN Human Rights Committee Concluding Observations 2015;[6]
- UN CRPD Committee Concluding Observations 2017;[7]
- UN Human Rights Committee General Comment No 16 1988;[8]
- UN CAT Committee General Comment No 3 2012;[9]
- UN CRPD Committee General Comment No 1 2014;[10]
- UN Special Rapporteur on the Right to Privacy, Professor

---

[1] Ratified by the UK in 1951.
[2] Ratified by the UK in 1976.
[3] Ratified by the UK in 1991.
[4] Ratified by the UK in 2009.
[5] Ratified by the UK in 1987.
[6] CCPR/C/GBR/CO/7, Human Rights Committee, 'Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland,' 23 July 2015.
[7] CRPD/C/GBR/CO/1, Committee on the Rights of Persons with Disabilities 'Concluding observations on the initial report of the United Kingdom of Great Britain and Northern Ireland', 29th August 2017.
[8] Human Rights Committee, 'General Comment No 16: Article 17 (Right to Privacy)', (1988).
[9] CAT/C/GC/3 Committee against Torture, 'General Comment No 3; Implementation of Article 14 by States Parties', 13 December 2012.
[10] CRPD/C/GC/1, Committee on the Rights of Persons with Disabilities, 'General Comment No 1, Article 12: Equal Recognition before the Law', 31st March-11th April 2014.

Joseph Cannataci, Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland 2018.[11]

1.4 The NIHRC welcomes the opportunity to give its views to the Department of Justice (DoJ) on a Legislative Consent Motion (LCM) to bring provisions from the Policing, Crime, Sentencing and Courts Bill into effect in Northern Ireland. The NIHRC acknowledges that the DoJ requested the Commission's views specifically on the extraction of data from electronic devices but notes that there are other points within the draft Bill that should be given further attention in relation to human rights compliance.

2.0 Human Rights Standards

The duty to protect from harm

2.1 The UK is required, under its international obligations, to respect, protect and fulfil the human rights of those under its jurisdiction. Often this will require that the State put in place a robust legal framework to ensure that individuals rights are protected. Specific positive obligations to protect arise under the right to life, under Article 2 ECHR, and the prohibition on torture, inhuman and degrading treatment, under Article 3 ECHR.[12] This includes an investigative obligation, requiring an effective, official investigation into allegations of harm. Such an investigation, under Articles 2 or 3 ECHR, should be independent and of the State's own motion, be capable of identifying those responsible, be prompt and conducted with reasonable expedition and have a degree of public scrutiny and involvement of the victim or next of kin.[13]

2.2 While the ECHR applies to all persons irrespective of age, the UN Convention on the Rights of the Child highlights the principle that the 'best interests' of the child are paramount. Article 19(1) UNCRC also requires the State to protect a child from "all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse".

2.3 Human rights law recognises the importance of protecting victims of human rights abuses from secondary victimisation. The UN has identified that secondary victimisation is most "apparent within the criminal justice system"[14] and that "preventing repeat victimisation can be a powerful way not only to reduce overall victimisation but also to speed the victim's

[11] Special Rapporteur on Privacy, Professor Joseph Cannataci, 'End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland' 29 June 2018.
[12] See also Articles 6 and 7 ICCPR; UNCAT.
[13] Jordan v. the United Kingdom, Application No. 24746/96 (4 August 2001) paras 106-9.
[14] UNODC, Handbook on Justice for Victims on the use and application of the Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power, p.9.

psychological recovery."[15] The UN Committee against Torture recognises re-traumatisation and requires that a victim who has suffered violence or trauma "should benefit from adequate care and protection to avoid his or her re-traumatisation in the course of legal and administrative procedures".[16]

The right to private and family life

2.4 The right to respect for private and family life is protected by Article 17 ICCPR and Article 8 of the ECHR. The UNCRPD and UNCRC also contain similar provisions.[17] These provisions are qualified in nature and recognise that restrictions on this right are permissible in certain circumstances.

2.5 The European Court of Human Rights (ECt.HR) jurisprudence has reflected that the storing of an individual's information relating to their private life by a public authority amounts to an interference with article 8.[18] The subsequent use of the stored information does not affect that finding.[19] The ECt.HR notes that the term 'private life' is broad and "not susceptible to exhaustive definition" and can therefore embrace multiple aspects of a person's physical and social identity.[20] In determining whether personal information retained by public authorities relates to an individual's private life, the ECt.HR will have due regard for the context in which the information has been recorded, the nature of the records, the way they have been used or processed and the results that may be obtained.[21]

2.6 The ECt.HR will provide a margin of appreciation to States in relation to qualified rights, such as Article 8. States have a certain amount of discretion in how they choose to limit certain rights where there is a need to do so.[22] However, any limitation to Article 8 must be necessary and proportionate in line with Article 8(2).

2.7 The UN Human Rights Committee (HRC) notes, in its General Comment No 16 on Article 17, that the gathering and holding of personal information and data by public authorities must be regulated by law.[23] The HRC further notes that, in order to have the most effective protection of privacy, "every individual should also be able to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes".[24]

---

[15] UNODC, 'Handbook on Justice for Victims on the use and application of the Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power', p. iv and 50.
[16] CAT/C/GC/3 Committee against Torture, 'General Comment No 3; Implementation of Article 14 by States Parties', 13 December 2012, at para 21.
[17] Article 16 UNCRC; Article 22 UNCRPD.
[18] Leander v Sweden (1987) 9 EHRR 433.
[19] Amann v Switzerland (2000) ECHR 88.
[20] S and Marper v The United Kingdom (2008) ECHR 1581, at para 66.
[21] Ibid, at para 67.
[22] Dudgeon v UK (1981) ECHR 5, at paras 51-53.
[23] Human Rights Committee, 'General Comment No 16: Article 17 (Right to Privacy)', (1988), at para 10.
[24] Ibid.

2.8 The UN General Assembly (UNGA) has emphasised that the arbitrary collection of data is a highly intrusive act and violates the right to privacy and can interfere with the right to freedom of expression and "may contradict the tenets of a democratic society".[25] The UNGA further notes that concerns about public security may justify the extraction of sensitive information, but States must ensure full compliance with international human rights obligations.[26] In 2018, the Special Rapporteur on Privacy identified his concerns regarding UK intelligence and law enforcement agencies obtaining "bulk data" in order to prevent or investigate crime, noting there are less intrusive measures available.[27]

2.9 In its concluding observations on the United Kingdom, the Human Rights Committee has previously advised the UK Government that "measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity".[28]

2.10 Article 1 of the Council of Europe Convention 108 on the Protection of Individuals with Regard to the Processing of Personal Data states that the object and purpose of the Convention is to "secure … for every individual... respect for his rights and fundamental freedoms, in particular his right to privacy, with regard to the automatic processing of personal data".

3.0 Background to Data Extraction from Electronic Devices

3.1 Rapid technological development has enabled individuals to use new information and communication technologies in a way that was not previously possible. Consequently, this has enhanced the capacity of state agencies to undertake surveillance, interception and data collection.[29]

3.2 Electronic devices, namely mobile phones, have become "repositories of our personal information, generating huge amounts of data".[30] Subsequently, digital evidence from electronic devices is being increasingly used in criminal investigations, with police not only collecting this evidence from suspects, but also victims.[31]

---

[25] A/RES/71/199, UN General Assembly, 'The Right to Privacy in the Digital Age', 25 January 2017.
[26] Ibid.
[27] Special Rapporteur on Privacy, Professor Joseph Cannataci, 'End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland' 29 June 2018.
[28] CCPR/C/GBR/CO/7, Human Rights Committee, 'Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland,' 23 July 2015
[29] A/RES/71/199, UN General Assembly, 'The Right to Privacy in the Digital Age', 25 January 2017.
[30] Information Commissioner's Office, 'Mobile Phone Data Extraction by Police Forces in England and Wales: Investigation Report' (ICO, 2020), at 7.
[31] Big Brother Watch, 'Digital Strip Searches: The Police Data Investigations of Victims', (2019).

3.3 The Commission recognises the investigation of the Information Commissioner into mobile phone extraction (MPE). This followed concerns that police forces were inconsistent in their approach to MPE, that there were poor practices in information handling including overly wide data extraction practices, and a reliance on consent as the basis for undertaking MPE in circumstances where it was not appropriate.[32] One of the recommendations following this investigation identified the need for "better rules, ideally set out in a statutory code of practice, that will provide greater clarity and foreseeability about when, why and how the police and other law enforcement agencies use MPE".[33]

3.4 The UK government intends to implement this recommendation through the Policing, Crime, Sentencing and Courts Bill. Section 36(1) of the Bill identifies that authorised persons can extract information from an electronic device if the user has voluntarily provided the device and the user has agreed to the extraction of information. Section 36(2) of the Bill identifies that powers described in subsection (1) may only be exercised for the purposes of preventing, detecting, investigating or prosecuting crime, to locate a missing person or to protect a child or an at-risk adult from physical, emotional or mental harm. Section 39 of the Bill allows for the extraction of information from an electronic device used by a person who has died for the purposes of an investigation into the person's death. Section 36(2) creates provisions to allow authorised persons to intervene to prevent deaths and effectively investigate crimes.

3.5 Section 37(1) of the Bill identifies that a child is not capable of consenting to provide electronic devices for the purposes of data extraction, while sections 37(2) and (3) identify that a parent or guardian, a relevant authority, a responsible person over the age of 18 or any other relevant authorised person may consent on a child's behalf. Article 3 of the UN CRC states that "in all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration". Section 37 ensures that authorised persons have the powers to extract data from an electronic device belonging to a child for the purposes listed in Section 36(2).

3.6 The Commission notes that for the purposes of this Bill, a child is defined as a person under the age of 16. Article 1 of the UN CRC identifies that a child means "a human being below the age of 18 years".

3.7 Section 37(6) of the Bill identifies that an adult without capacity cannot voluntarily provide an electronic device to an authorised person or agree to the purposes of the extraction of data. Article 12 of the UN Convention on the Rights of Persons with Disabilities (UN CRPD) states that all "persons

---

[32] Information Commissioner's Office, 'Mobile Phone Data Extraction by Police Forces in England and Wales: Investigation Report' (ICO, 2020), at 7.
[33] Ibid at 9.

with disabilities have the right to recognition everywhere as persons before the law", and States Parties should "take all appropriate measures to provide access to persons with disabilities to the support they may require in exercising their legal capacity". In General Comment No 1, the Committee on the Rights of Persons with Disabilities (CRPD) note that persons with disabilities remain the most common group whose legal capacity is denied. The CRPD further state that "the right to equal recognition before the law implies that legal capacity is a universal attribute inherent in all persons by virtue of their humanity and must be upheld for persons with disabilities on an equal basis with others".[34] In its concluding observations on the United Kingdom, the CRPD notes its concern that UK legislation restricts the legal capacity of persons with disabilities on the basis of perceived impairment.[35] Any limitation to a person's legal capacity interferes with their right to equal recognition before the law.

3.8 Section 37(3)(b) identifies that, in the event that an authorised person under section 37(3)(a) is not available to consent to the extraction of data "any responsible person who is aged 18 or over" may consent to the extraction of data from an electronic device belonging to a child. The same provision for adults without capacity is identified in section 37(8)(f). These provisions are extremely broad given the lack of guidance on what constitutes a responsible person over the age of 18. Section 37(5) states:

> If an authorised person ("A") exercises the power under section 36(1) as a result of action taken under subsection (2) by a person within subsection (3)(b), A must, unless A considers that it is not appropriate to do so, inform a person within subsection (3)(a) that A has exercised the power.

There is no further guidance on what may constitute an appropriate reason not to inform a person under subsection 3(a) that consent has been given by a person under subsection (3)(b) to extract data from an electronic device belonging to a child in their care. These are provisions that require further explanation, potentially through the code of practice, to ensure their compliance with human rights standards.

3.9 The Bill does not identify what might happen in the event that an individual does not give consent, except in Section 36(9), which notes 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".

---

[34] CRPD/C/GC/1, Committee on the Rights of Persons with Disabilities, 'General Comment No 1, Article 12: Equal Recognition before the Law', 31st March-11th April 2014, at para 8.
[35] CRPD/C/GBR/CO/1, Committee on the Rights of Persons with Disabilities 'Concluding observations on the initial report of the United Kingdom of Great Britain and Northern Ireland', 29th August 2017, at para 30(a).

3.10 Chapter 3 refers to "authorised persons" in relation to data extraction from electronic devices. Section 42 identifies authorised persons means a person listed in Schedule 3. Schedule 3 contains a list of authorised persons, including the National Crime Agency. The Commission notes that all persons listed under Schedule 3 must be subject to oversight mechanisms to ensure they act in compliance with legislation and statutory guidance on mobile data extraction. For the purposes of such organisations operating in NI, this should include in appropriate circumstances scrutiny by the NI Policing Board.

3.11 The Commission recognises the intention of Chapter 3 of the Bill is to ensure legal clarity for public authorities who are interfering with individuals' right to privacy and for the individuals who are potentially going to consent to have their personal data extracted from electronic devices. However, the Commission remains concerned that this provision lacks legal certainty, specifically in relation to a statutory code of practice and the extent of the data extraction in investigating and prosecuting sexual assault cases.

3.12 **The NIHRC advises that the proposed Code of Practice should be published and consulted on in advance of the LCM to ensure its compliance with human rights standards. Subject to review of the code of practice, the NIHRC advises that an LCM would be appropriate to bring this chapter of the Police, Crime, Sentencing and Crime to the NI Assembly.**

3.13 **The NIHRC recommends that any individual or organisation listed as an "authorised person" in Schedule 3 of the Bill with jurisdiction in NI should be subject to specific oversight and required to publish the extent of the use of the powers and their circumstances.**

4.0 Code of Practice

4.1 Section 40 of the Police, Crime, Sentencing and Courts Bill identifies that the Secretary of State for the Home Department must prepare a code of practice containing guidance on the exercise of powers under sections 36 and 39 of the Bill. The code of practice must be prepared in consultation with the Information Commissioner, Scottish Ministers, the Department of Justice in Northern Ireland and other persons as the Secretary of State believes appropriate.

4.2 Issues around data extraction are particularly pertinent to marginalised groups, including women, children, LGBTQ+ communities and other

vulnerable groups.[36] Accordingly, consultation with individuals and organisations representing these communities is important to ensuring policies on data extraction do not have disproportionate, negative impacts on these groups. If this statutory guidance is applicable to police forces in NI, it is appropriate to allow for public consultation with the wider NI population

4.3 **The NIHRC recommends that any statutory code of practice in relation to data extraction from electronic devices which is applicable to NI should be produced in consultation with individuals and relevant organisations in NI.**

4.4 The Home Office has released a fact sheet concerning the proposed statutory code of practice. It identifies that the code of practice will give "practical guidance to authorities on the use of the power, including how to determine which legal power to use in the circumstances and how they should confirm that extraction of that information is necessary and proportionate." The fact sheet also identifies that the code of practice will emphasise the use of other, less intrusive methods of evidence gathering will be considered before extracting data from individuals' electronic devices.[37]

4.5 The qualified nature of Article 8(2) ECHR permits interference with the right to privacy by public authorities only as far as "is necessary in a democratic society". The UN HRC notes, that in order to have effective protection for privacy, individuals must be aware of precisely what information is being held about them.[38] Legal certainty is required of the proposed Code of Practice to ensure that public authorities operate in compliance with human rights standards. Any code of practice dealing with data extraction from electronic devices should expressly set out how Article 8 ECHR considerations are taken into account through the decision making process and provide sufficient safeguards to ensure these powers are only used in so far as is necessary.

4.6 **The NIHRC recommends the proposed statutory code of practice should provide sufficient detailed guidance to enable those making decisions on the extraction of data from electronic devices to do so in an ECHR compliant manner.**

5.0 Data Extraction and Victims of Sexual Assault

[36] UN General Assembly, 'Right to Privacy: Report of the Special Rapporteur on the Right to Privacy', Fortieth Session, 25th February-22nd March 2019, at paras 48-49.
[37] UK Government, 'Police, Crime, Sentencing and Courts Bill 2021: Data Extraction Factsheet', Available at Police, Crime, Sentencing and Courts Bill 2021: data extraction factsheet - GOV.UK (www.gov.uk)
[38] Human Rights Committee, 'General Comment No 16: Article 17 (Right to Privacy)', (1988), at para 10.

5.1 Big Brother Watch noted that the practice of obtaining data from victims' phones is "almost exclusively" being used in cases concerning sexual assault.[39] Big Brother Watch conducted a freedom of information survey, with 100% of respondent police forces identifying that they had taken digital information from complainants of sexual offences' mobile phones.[40]

5.2 Given the scale of the information that is accumulated through data extraction from electronic devices, there have been criticisms over lengthy delays in prosecuting sexual assault offences. A survey by Big Brother Watch identified that demands on police to examine digital devices for evidence gathering in England and Wales led to police being overwhelmed, with delays of up to six months for digital devices to be examined.[41] It is estimated that collecting excessive amounts of data in England and Wales is causing overall delays of up to 18 months to criminal cases.[42] In NI, the Public Prosecution Service have indicated that decisions regarding prosecutions of sexual assault offences take on average 255 days, around 8 months.[43] New legislation has not addressed issues around delays to prosecutions as a consequence of data extraction.

5.3 In 2019, in response to criticism regarding the extent of the extraction of data from sexual assault victims' electronic devices, the National Police Chiefs' Council released Digital Processing Notices for use by police in England and Wales as a way to obtain victims' consent to extract personal data.[44] These notices themselves have received widespread criticism, with the Victims Commissioner for England and Wales noting that instead of creating more proportionate demands for sexual assault victims' data, "it levelled up, so that more data was required by some forces who had previously asked for less".[45]

5.4 As a result of data extraction practices, many victims of sexual assault have identified that they felt they had to choose between disclosing all of the personal information contained on their digital devices or accessing justice.[46] This was retraumatising for many victims, who felt that the police were "more interested in investigating them over investigating the defendant".[47] These data extraction policies were not in keeping with judicial Protocol on the disclosure of unused material in criminal cases, which states that:

> Victims do not waive... their right to privacy under article 8 of the ECHR, by making a complaint against the accused. The court, as a public authority, must ensure that any interference with the right to

---

[39] Big Brother Watch, 'Digital Strip Searches: The Police Data Investigations of Victims', (2019), at 8.
[40] Ibid
[41] Ibid, at 18.
[42] Ibid.
[43] NI Statistics and Research Agency, 'Statistical Bulletin: Cases Involving Sexual Offences 2019/20' (NISRA, 2020).
[44] Big Brother Watch, 'Digital Strip Searches: The Police Data Investigations of Victims', (2019), at 9.
[45] Victims Commissioner for England and Wales, 'Police and CPS scrap digital extraction forms for rap cases', (2020).
[46] Ibid.
[47] Ibid.

privacy under article 8 is in accordance with the law, and is necessary in pursuit of a legitimate public interest.[48]

After a legal challenge by the Centre for Women's Justice, which argued the use of these forms was unlawful, discriminatory and led to excessive and intrusive disclosure requests, the National Police Chiefs' Council withdrew the use of Digital Processing Notices in England and Wales.[49]

5.5 The Court of Appeal decision in *R v Bater-James* has provided a set of legal principles for the lawful and proportionate approach to the disclosure of complainants' data in rape and sexual offence cases. The case concerned two appeals, where both appellants had been convicted of sexual offences but maintained that data from victims' electronic devices should have been allowed to be used as evidence in their respective trials.[50] The Court identified four issues of principle in relation to the use of victims' data in sexual offence trials; identifying circumstances when it is necessary for investigators to seek details of a witness' digital communications, how should the review of witness' electronic communications be conducted, what reassurance should be provided to the complainant as to the ambit of the review and the disclosure of relevant data, and what is the consequence if the complainant refuses to allow access to potentially relevant information.[51]

5.6 Any proposed code of practice should reference the judgement in *R v Bater-James* and consider the four issues of principle within its approach. The code of practice should provide guidance on how public authorities should incorporate the four issues of principle into their procedures when dealing with data extraction to ensure consistency of provision across police forces. Further consideration will be required as to how a code of practice will be provided for in NI, including to ensure that service provision is consistent across the UK jurisdictions.

5.7 **The NIHRC advises that the Code of Practice should expressly address the unique impact data extraction has had on sexual assault cases and the legal guidance from *R v Bater-James* should be incorporated into the code to ensure legal certainty.**

---

[48] Judicial Protocol of the Disclosure of Unused Material in Criminal Cases (2013), at para 47.
[49] Centre for Women's Justice, 'Controversial "consent forms" used in rpae and sexual assault cases withdrawn by police', available at Controversial 'consent forms' used in rape and sexual offences cases withdrawn by the police — Centre for Women's Justice
[50] R v Bater-James and Mohammad [2020] EWCA Crim 790
[51] Ibid, at 65.

Contact us

www.nihrc.org | info@nihrc.org | +44 (0)28 9024 3987
4th Floor, Alfred House, 19-21 Alfred Street, Belfast, BT2 8ED