Written evidence submitted by Judith Ratcliffe, Privacy Professional and UK Citizen (CPB24)

Proposed Crime and Policing Bill amendments

1) Add a legal definition of *extortion* into Law and make sure it includes:

Making it a criminal offence *(with strict liability compensation to be handed directly to any affected individuals)* to*:*

a) *Demand and/or receive payment for actioning, upholding and/or respecting a person's Fundamental Human Rights, including, Privacy Rights;*

b) *attempt to appropriate, extinguish or limit people's Rights, including, but not limited to, in exchange for access to essential products and essential services;*

c) *demand personal data 'with menaces' (e.g. TV Licensing);*

d) *demand money for services that people aren't using/ don't use (e.g. TV Licensing);*

e) *deny people access to essential products and essential services (whether from Public Authorities or Private /Commercial /Not-For-Proft or any other type of organisation/ company or institution), where those people refuse to consent to giving away data/ giving up data protection rights, giving up privacy rights, giving up any or all aspects of their privacy (including personal autonomy, for example);*

f) *trick, manipulate, people into consenting to giving away data/ giving up data protection rights, giving up privacy rights, giving up any or all aspects of their privacy (including personal autonomy, for example), including, but not limited to, in exchange for access to essential products and essential services.*

g) *encourage, or, force people to consent to giving away data/ giving up data protection rights, giving up privacy rights, giving up any or all aspects of their privacy (including personal autonomy, for example), including, but not limited to, in exchange for access to essential products and essential services.*

Include express prohibitions on:

i) *Obtaining data (whether from the individuals themselves or from any other source), including contact details and names, and anything else, about people who are not your customers, with the intention of demanding money for products or services (Hint/ explanatory note- if they aren't your customers, so don't use your products or services – you cannot demand that they pay you for your products or services, or that they identify themselves to your organisation in any way);*

ii) Sending communications demanding money, (unless you know for a fact that the people to whom you send those communications) use your products/ services and haven't paid you in a timely manner, despite bills being raise in the proper legal way (without menaces).

iii) Demanding money for providing paper bills or other paper communications/ paper-based interactions, paper bank statements and/or any other paper-based part of essential services (even if organisations/ Government Departments are engaged in 'drives to digital').

2) Amend the Police and Criminal Evidence Act, and all other Policing/ Law Enforcement / Intelligence Services Law as follows:

*The use of facial recognition, voice recognition, gait recognition is **banned** from all public law enforcement activities.*

Reason for amendment: Facial Recognition and Voice Recognition, in particular have been shown to present the innocent as guilty on numerous, documented, occasions. They appear to do nothing to assist in identifying genuine offenders. Ordinary CCTV is generally enough to identify offenders, where film/ photo footage is necessary. Facial Recognition fails to enhance this.

3) **Amend the Police and Criminal Evidence Act, and all other Policing/ Law Enforcement / Intelligence Services Law as follows:**

Bodycameras must *not* be used (including in public transport and any other public area) by anyone except fully trained police officers and intelligence services staff.

Reason for amendment: There have been a number of instances on trains, where managers have recorded the voices of passengers who were using the toilet facilities and then filmed them on bodycameras as they exited those facilities – This was an abuse of power and position and resulted in those passengers feeling traumatised and reluctant to engage in further train travel as a result - Those passengers had valid tickets. Those passengers were behaving properly and legally at all times. There was no valid reason for recording their voices or filming them on bodycameras. The train companies concerned refused to promptly destroy footage or to provide any other means of redress or restitution. A clear and unequivocal message needs to be sent that abusing passengers will *not* be tolerated.

To stop passengers being filmed abusively by train staff, the technology used must be removed from use.

There is no need for bodycameras as there is more than enough CCTV on trains and in stations that could/ should be used instead.

4) **Amend the Police and Criminal Evidence Act, and all other Policing/ Law Enforcement / Intelligence Services Law as follows:**

Abusing Passengers is strictly prohibited – anyone found guilty of abusing passengers *(including by filming them/ recording their voices when using or exiting toilet facilities)* will be sentenced to a minimum of 6 months to 1 year in prison (depending on the nature and severity of the offence) and fined £10,000. Such money to be given in compensation to the victim to acknowledge the trauma such offences can cause.

Reason for amendment: There have been a number of instances on trains, where managers have behaved abusively towards passengers, including inappropriate filming on bodycameras, in circumstances when they knew or should reasonably have been aware that someone was innocent. There have been instances when Transport For London staff acting in concert with police officers appear to have conspired to falsely imprison people on buses and there have been other instances too of Transport For London staff apparently abusing their powers. They often appear even to fail to identify themselves properly to passengers.

Little to no effective redress seems to be forthcoming when such powers are abused, which appears to mean that organisations will allow passengers to be abused over and over again.

The adverse effects on passengers, include making them afraid to use public transport and subsequent adverse effects on the environment may be the result, where people feel that their only option to escape unlawful persecution is to travel privately.

A clear and unequivocal message needs to be sent that abusing passengers will *not* be tolerated.

5) **Amend the Police and Criminal Evidence Act, and all other Policing/ Law Enforcement / Intelligence Services Law as follows:**

Abusing customers / service users is strictly prohibited.

Reason for amendment: Threatening signs have appeared everywhere threatening innocent people and telling them *not* to abuse staff – A number of staff members at organisations appear to take this as an invitation to abuse customers/ service users – and then trying to claim that those customers/ service users have been ‘abusive’ when those customers/ service users raise reasonable and polite, but firm complaints.

Changes need to be made to all legislation to confirm:

a) That firm but polite complaints *don’t* count as being abusive.

b) That people have the Right to complain about poor service, bad staff conduct and similar and that making such complaints does *not* in and of itself make customers abusive.

c) **That staff must *not* abuse customers/ service users and if they raise their voices to them, or in any way act abusively towards them, that customers/ service users can in their turn, receive immediate compensation for that behaviour of a set amount that is sufficiently high to act as a deterrent against such behaviour**.

6) **Amend the Police and Criminal Evidence Act, and all other Policing/ Law Enforcement / Intelligence Services Law as follows:**

Where a police officer knows or should reasonably be aware that they have (whether accidentally or otherwise) recorded an innocent person using a bodycamera they must, immediately, provide the individual they recorded with a written record of their own name, where they are based, their immediate line manager and (above all), destroy the footage immediately, in the presence of the individual recorded. If footage cannot be destroyed immediately (which should be in exceptional circumstances), they must destroy the footage within an absolute maximum of 24 hours after the unlawful recording has happened. They must provide written confirmation of such destruction, preferably immediately, but, if not, then within an absolute maximum of 1 week after destruction has happened.

Reason for the amendment: There has been abuse of bodycameras by police officers on public transport – they recorded innocent individuals, unlawfully and then refused to destroy the data, promptly. They also failed to identify themselves to those individuals, making it more difficult to gain redress or to hold them accountable for their bad actions.

7) Amend the Police and Criminal Evidence Act, and all other Policing/ Law Enforcement / Intelligence Services Law as follows:

Police forces must erase all person data belonging to innocent persons from the Police National Computer with immediate effect.

They must *not* even keep ‘pseudonymised’ data because even ‘pseudonymised’ data can be used to re-identify someone and can cause them harm.

Destroy equals the equivalent of burning to ashes.

Police forces must *not* upload innocent persons’ data to the police national computer.

Police forces must *not* use innocent persons' data for building or testing AI/ algorithms, systems or any other form of testing, analytics or anything else – They must take all reasonable steps to avoid collecting data of innocent persons and within an absolute maximum of 48 hours after collecting the data of people they then realise are innocent, they must destroy that data. No copies of that data can be kept.

The same applies to the Intelligence Services.

Reason for amendments:

Treating innocent people as though they are guilty undermines Public confidence in the police and makes them less likely to report crimes or to co-operate with enquiries for fear of themselves becoming suspect.

The Intelligence Services Codes of Conduct propose using personal data (including of innocent persons) to create Generative AI – this puts people at immediate risk of potentially irrevocable harm – they lose control of their data the moment the intelligence services scrape it from, e.g. the internet and may be mistaken for terrorists in worst case scenarios – this could lead to unfair incarceration or even death.

Problems include the lack of information given to individuals about what is happening to their data and the lack of ability to get Rights actioned in respect of it.

8) **Amendments to the Police, Crime, Sentencing and Courts Act, 2022**
The following additions are recommended:

9) **Part A1A – SERIOUS OFFENCES RELATING TO MINISTERS, CIVIL SERVANTS, THE NATIONAL HEALTH SERVICE, EMPLOYER and PHARMACEUTICAL COMPANIES, PUBLIC SERVICE (AND OTHER) BROADCASTERS and MEMBERS OF THE PRESS**

1 It shall be an offence for any of the above-mentioned parties to

a) Infringe the Article 2 ECHR/HRA 1998 Right to Life of any UK, or International Citizen, including those who are homeless/awaiting immigration decisions.

b) Mandate (or encourage the mandation of) any form of vaccine or medical treatment which could cause death or serious harm (including allergic reactions or other side effects)

c) Dismiss (or cause to be dismissed) any person because they have refused a vaccine or medical treatment or Refuse someone work because they have refused a vaccine or medical treatment

d) Incite hate crimes and discrimination about, or, towards any person who refuses to have a vaccine or medical treatment

e) Refuse (or cause to be refused) any person entry to any public place/shop/ place of entertainment because they refuse to have a vaccine/medical treatment

2 It shall be a serious offence for MINISTERS, CIVIL SERVANTS, THE NATIONAL HEALTH SERVICE, EMPLOYER and PHARMACEUTICAL COMPANIES, PUBLIC SERVICE (AND OTHER) BROADCASTERS and MEMBERS OF THE PRESS to

a) Whitewash, ignore, deliberately turn a blind eye to, conceal, or, fail to make clearly and widely known to the UK Public, dangers and health risks/ risks to life/ risks of serious harm of vaccines and other medical treatments.

b) Down-play any such risks to life/ risks of serious harm.

c) Hush up any such risks to life/ risks of serious harm.

d) Label any critics e.g. as anti-vaxxers in order to close down any disagreement/ dissent.

10) Part A2A – SERIOUS OFFENCES RELATING TO DRONES

1 It shall be an offence to fly any drones which have video recording/sound recording equipment attached to them

a) over back gardens and houses

b) over members of the public who are innocently going about their daily business

Unless they have the express and explicit consent of the homeowners/ members of the public who they intend to record.

11) Part A3A – OFFENCES RELATING TO RECORDING SOUND IN SHOPS

1 It shall be an offence to record the voices of customers, particularly in healthcare shops such as, for example, Boots. It shall particularly also be an offence where those customers serve parents with young children who accompany them while shopping.

The UK Public have the Right to go about their daily lives, without being suspected or accused of criminal activity, of which they are entirely innocent. They have the Right NOT to be treated like criminals. They also have the Right not to have their health data (including details of prescriptions/ unprescribed medicines) recorded when the sole purpose of their entry into a shop is to pick up a prescription or to buy unprescribed medicines. They have the Right to be left alone and not to have their private lives interfered with by the state or by businesses.

12) **Part2-Prevention, investigating and prosecution of crime. Chapter 1 – Functions Relation to Serious Violence**

9 Power to authorise collaboration etc. with other persons

5 (a) would contravene Privacy Law and/or the Data Protection Legislation (~~but in determining whether a disclosure would do so, any power conferred by the regulations is to be taken into account~~), or

9 In this Chapter "Privacy Law" has the same definition as set out in the European Convention on Human Rights (ECHR) and Human Rights Act (HRA) 1998, including the Right to respect for Private and Family Life, Home and Correspondence. In this Chapter "the Data Protection Legislation", means the UK-GDPR, the Data Protection Act 2018 (in so far as it complies with the UK-GDPR and upholds individuals rights and freedoms), PECR (the Privacy and Electronic Communications Regulations, 2003) and any upcoming European e-Privacy Regulation.

15 Disclosure of information

4 But this section does not authorise a disclosure of information that
(a) would contravene Privacy Law and/or the Data Protection Legislation ~~(but in determining whether a disclosure would do so, any power conferred by the regulations is to be taken into account~~), or

16 Supply of information to local policing bodies

(6) But subsection (4) does not require a disclosure of information that

(a) would contravene Privacy Law and/or the Data Protection Legislation (but in determining whether a disclosure would do so, any power conferred by the regulations is to be taken into account), or

29 Information: supplementary

(1) A person may **must** not be required under section 28 to disclose information that the person could not be compelled to disclose in proceedings before the high court.

(b) A person must not be required under section 28 to disclose information that they have a Right to withold under their Right to Remain Silent and, if a witness, Right NOT to self-incriminate.

(3) But sections 26-28 do not require or authorise a disclosure of information that -
(a) would contravene Privacy Law and/or the Data Protection Legislation, or the Common Law Right to Remain Silent (~~but in determining whether a disclosure would do so, any power conferred by the regulations is to be taken into account~~), or

(5) In this section: "Privacy Law" has the same definition as set out in the European Convention on Human Rights (ECHR) and Human Rights Act (HRA) 1998, including the Right to respect for Private and Family Life, Home and Correspondence. In this Chapter "the Data Protection Legislation", means the UK-GDPR, the Data Protection Act 2018 (in so far as it complies with the UK-GDPR and upholds individuals rights and freedoms), PECR (the Privacy and Electronic Communications Regulations, 2003) and any upcoming European e-Privacy Regulation.

13)**CHAPTER 3**
EXTRACTION OF INFORMATION FROM ELECTRONIC DEVICES

36 Extraction of information from electronic devices: investigations of crime etc

(1) An authorised person may extract information stored on an electronic device from that device if-

(a) a user of the device has voluntarily provided the device to an authorised person, and

(b) that user has agreed to the extraction of information from the device by an authorisation

(1A1) **Voluntarily** means that an individual must **not** have been
a) coerced or threatened
b) cajoled
c) bribed
d) or otherwise unduly influenced in any way

Into handing over their device.

Undue Influence/unduly influencing includes

a) threats/statements about not being prepared to/being unable to investigate further/ take a complaint seriously/escalate a complaint without using the data/ extracting the data from an individual's device (where the individual concerned is a victim)

b) threats/ statements about a person 'looking/appearing' guilty whether to the police or to a Court or any other party, if they refuse to hand over a device/ permit extraction of data.

(1B1)
(1) Any agreement to hand over a device/ to permit data extraction from a device

(a) **must** meet the Valid Consent Conditions set out in **Article 7 of the UK-GDPR and EU-GDPR** AND

(b) is also subject to and must meet the conditions for validly informing a person before/at the time of data collection, set out in **Article 13 of the UK-GDPR/EU-GDPR.**

(1C1)

(1) A Privacy Agreement signed by the authority taking the device and the data must be handed over to the individual before they are asked to agree to any taking of a device or extraction of data from it and if any of the terms appear to be unfair to the individual, they have the Right to strike through those terms and to refuse to agree to those exact terms, without any invalidation of the rest of the agreement.

(2) A Privacy Agreement signed by the authority taking the device and the data that confirms that conditions for limiting

a) the people who can access/view and process the data (and no sharing with unauthorised third parties). There is to be a strict limitation to those who 'need to know'.

b) where the data can be accessed/viewed and processed (e.g. solely within the UK and solely by Police Station Y, within Z Police Station).

b) the purpose for taking and using the data to the exact purposes set out within the agreement AND no others

c) the amount and type of data to be extracted

d) the retention period of
i) the device itself
ii) the data taken from the device

e) all of the other information that is required to be given under **Articles 13 and 14 of the UK-GDPR and EU-GDPR.**

(3) Within the Agreement there must also be a clause stating that any accidentally obtained and/or irrelevant data (e.g. data that has no bearing on the current investigation/case) will be immediately and irreversibly purged/deleted/destroyed (both paper and electronic copies) AND

(4) Within the Agreement there must also be a clause making it clear that none of the extracted data will be repurposed for any reason (used for anything other than the clearly and openly stated purposes in the Privacy Agreement), whether by the collectors of the data, or their processors/sub-processors/ any other third parties.

36 Extraction of information from electronic devices: investigations of crime etc

(5) An authorised person may exercise the power in subsection 1, only if -

(c) It has in place policies/processes and procedures for the collection, use, storage, correction and destruction of the desired information, which comply with Privacy Law and the Data Protection Legislation AND IT systems and Manual Systems which have been designed to permit the safe correction and destruction of such information in accordance with Privacy Law and the Data Protection Legislation, and which prevent automated decision-making and profiling which could have legal effects on an individual or otherwise significantly affect their ability to obtain a fair trial or a fair Law Enforcement Investigation.

(d) It complies with Data Protection Legislation and Cyber Security Guidelines to prevent infringements of Data Protection Legislation and Personal Data Breaches.

(9) 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- unless those enactments or rules of law break Privacy and Data Protection Law, in which case any such extraction/production/seizure/obtention will be unlawful.

37 Application of section 36 to children and adults without capacity

(1A1) **Voluntarily** means that an individual must **not** have been

a) coerced or threatened
b) cajoled
c) bribed
d) or otherwise unduly influenced in any way

Into handing over their device.

Undue Influence/unduly influencing includes
a) threats/statements about not being prepared to/being unable to investigate further/ take a complaint seriously/escalate a complaint without using the data/ extracting the data from an individual's device (where the individual concerned is a victim)

b) threats/ statements about a person 'looking/appearing' guilty whether to the police or to a Court or any other party, if they refuse to hand over a device/ permit extraction of data.

(1B1)
(1) Any agreement to hand over a device/ to permit data extraction from a device

(a) **must** meet the Valid Consent Conditions set out in **Article 7 of the UK-GDPR and EU-GDPR** AND

(b) is also subject to and must meet the conditions for validly informing a person before/at the time of data collection, set out in **Article 13 of the UK-GDPR/EU-GDPR.**

AND

(c) must write it in the language that/ explain it in such a way that a child (of the child in question's age and maturity) could understand it.

(1C1)

(1) A Privacy Agreement signed by the authority taking the device and the data must be handed over to the individual before they are asked to agree to any taking of a device or extraction of data from it and if any of the terms appear to be unfair to the individual, they have the Right to strike through those terms and to refuse to agree to those exact terms, without any invalidation of the rest of the agreement.

(2) A Privacy Agreement signed by the authority taking the device and the data that confirms that conditions for limiting

a) the people who can access/view and process the data (and no sharing with unauthorised third parties). There is to be a strict limitation to those who 'need to know'.

b) where the data can be accessed/viewed and processed (e.g. solely within the UK and solely by Police Station Y, within Z Police Station).

b) the purpose for taking and using the data to the exact purposes set out within the agreement AND no others

c) the amount and type of data to be extracted

d) the retention period of
i) the device itself
ii) the data taken from the device

e) all of the other information that is required to be given under **Articles 13 and 14 of the UK-GDPR and EU-GDPR.**

(3) Within the Agreement there must also be a clause stating that any accidentally obtained and/or irrelevant data (e.g. data that has no bearing on the current investigation/case) will be immediately and irreversibly purged/deleted/destroyed (both paper and electronic copies) AND

(4) Within the Agreement there must also be a clause making it clear that none of the extracted data will be repurposed for any reason (used for anything other than the clearly and openly stated purposes in the Privacy Agreement), whether by the collectors of the data, or their processors/sub-processors/ any other third parties.

37 Application of section 36 to children and adults without capacity

(2)

(c) It has in place policies/processes and procedures for the collection, use, storage, correction and destruction of the desired information, which comply with Privacy Law and the Data Protection Legislation AND IT systems and Manual Systems which have been designed to permit the safe correction and destruction of such information in accordance with Privacy Law and the Data Protection Legislation, and which prevent automated decision-making and profiling which could have legal effects on an individual or otherwise significantly affect their ability to obtain a fair trial or a fair Law Enforcement Investigation.

(d) It complies with Data Protection Legislation and Cyber Security Guidelines to prevent infringements of Data Protection Legislation and Personal Data Breaches.

(4)

(c) It has in place policies/processes and procedures for the collection, use, storage, correction and destruction of the desired information, which comply with Privacy Law and the Data Protection Legislation AND IT systems and Manual Systems which have been designed to permit the safe correction and destruction of such information in accordance with Privacy Law and the Data Protection Legislation, and which prevent automated decision-making and profiling which could have legal effects on an individual or otherwise significantly affect their ability to obtain a fair trial or a fair Law Enforcement Investigation.

(d) It complies with Data Protection Legislation and Cyber Security Guidelines to prevent infringements of Data Protection Legislation and Personal Data Breaches.

(5) Informing a person must comply with **Article 13 and Article 14 UK-GDPR and EU-GDPR requirements.**

(9)

(1A1) **Voluntarily** means that an individual must **not** have been

a) coerced or threatened

b) cajoled

c) bribed

d) or otherwise unduly influenced in any way

Into handing over their device.

Undue Influence/unduly influencing includes

a) threats/statements about not being prepared to/being unable to investigate further/ take a complaint seriously/escalate a complaint without using the data/ extracting the data from an individual's device (where the individual concerned is a victim)

b) threats/ statements about a person 'looking/appearing' guilty whether to the police or to a Court or any other party, if they refuse to hand over a device/ permit extraction of data.

(1B1)
(1) Any agreement to hand over a device/ to permit data extraction from a device

(a) **must** meet the Valid Consent Conditions set out in **Article 7 of the UK-GDPR and EU-GDPR** AND

(b) is also subject to and must meet the conditions for validly informing a person before/at the time of data collection, set out in **Article 13 of the UK-GDPR/EU-GDPR.**

AND

(c) must write it in the language that/ explain it in such a way that a child or an adult without capacity (of the child /adult in question's age and maturity) could understand it.

(1C1)

(1) A Privacy Agreement signed by the authority taking the device and the data must be handed over to the individual before they are asked to agree to any taking of a device or extraction of data from it and if any of the terms appear to be unfair to the individual, they have the Right to strike through those terms and to refuse to agree to those exact terms, without any invalidation of the rest of the agreement.

(2) A Privacy Agreement signed by the authority taking the device and the data that confirms that conditions for limiting

a) the people who can access/view and process the data (and no sharing with unauthorised third parties). There is to be a strict limitation to those who 'need to know'.

b) where the data can be accessed/viewed and processed (e.g. solely within the UK and solely by Police Station Y, within Z Police Station).

b) the purpose for taking and using the data to the exact purposes set out within the agreement AND no others

c) the amount and type of data to be extracted

d) the retention period of
i) the device itself
ii) the data taken from the device

e) all of the other information that is required to be given under **Articles 13 and 14 of the UK-GDPR and EU-GDPR.**

(3) Within the Agreement there must also be a clause stating that any accidentally obtained and/or irrelevant data (e.g. data that has no bearing on the current investigation/case) will be immediately and irreversibly purged/deleted/destroyed (both paper and electronic copies) AND

(4) Within the Agreement there must also be a clause making it clear that none of the extracted data will be repurposed for any reason (used for anything other than the clearly and openly stated purposes in the Privacy Agreement), whether by the collectors of the data, or their processors/sub-processors/ any other third parties.

38A1A The Data of Other Individuals on Devices Obtained by the Police/ within Data Extracted:

The data of individuals not involved in the case/ investigation must not be extracted from the device. These individuals must be permitted their full range of rights as set out in the Data Protection Legislation and have a Right to be Informed if their Data is obtained for any reason, in line with Section 36/37 of this Act and in line with the Data Protection Legislation.

For individuals involved in the case (where they are not the device's owner, but appear in anything on the device), they must be informed in the same way as the individual to whom the device belongs, in accordance with Privacy Law and Data Protection Legislation.

These individuals must be permitted their full range of rights as set out in the Data Protection Legislation and have a Right to be Informed if their Data is obtained for any reason, in line with Section 36/37 of this Act and in line with the Data Protection Legislation.

38 Application of section 36 where user has died etc

1A1 Under these circumstances section 36/ 37 applies to the next of kin/whoever holds the device on behalf of the individual, so long as that person is an individual and not a Law Enforcement Entity.

Where there is no investigation into the death of the user it shall not be lawful for a Law Enforcement Entity to retain/ obtain the device or to extract any data from the device.

The data of individuals not involved in the case/ investigation must not be extracted from the device.

These individuals must be permitted their full range of rights as set out in the Data Protection Legislation and have a Right to be Informed if their Data is obtained for any reason, in line with Section 36/37 of this Act and in line with the Data Protection Legislation.

For individuals involved in the case (where they are not the device's owner, but appear in anything on the device), they must be informed in the same way as the individual to whom the device belongs, in accordance with Privacy Law and Data Protection Legislation.

These individuals must be permitted their full range of rights as set out in the Data Protection Legislation and have a Right to be Informed if their Data is obtained for any reason, in line with Section 36/37 of this Act and in line with the Data Protection Legislation.

39 Extraction of information from electronic devices: investigations of death

1A1 The data of individuals not involved in the case/ investigation must not be extracted from the device. These individuals must be permitted their full range of rights as set out in the Data Protection Legislation and have a Right to be Informed if their Data is obtained for any reason, in line with Section 36/37 of this Act and in line with the Data Protection Legislation.

For individuals involved in the case (where they are not the device's owner, but appear in anything on the device), they must be informed in the same way as the individual to whom the device belongs, in accordance with Privacy Law and Data Protection Legislation.

These individuals must be permitted their full range of rights as set out in the Data Protection Legislation and have a Right to be Informed if their Data is obtained for any reason, in line with Section 36/37 of this Act and in line with the Data Protection Legislation.

22/03/2025