APPROVED
REDACTED

AN ARD-CHÚIRT
THE HIGH COURT

[2024] IEHC 721

Record No. 2024/155JR

BETWEEN/

YAVOR POPTOSHEV

APPLICANT

-AND-

THE DIRECTOR OF PUBLIC PROSECUTIONS, THE COMMISSIONER OF AN GARDA SÍOCHÁNA, IRELAND AND THE ATTORNEY GENERAL

RESPONDENTS

JUDGMENT of Mr. Justice Conleth Bradley delivered on the 11th day of December 2024

INTRODUCTION

Preliminary

1. In this application for judicial review, Mr. Poptoshev ("the applicant") seeks to challenge the provisions of section 48 of the Criminal Justice (Theft and Fraud Offences) Act 2001 ("the 2001 Act"),[1] which, in summary, allows a member of An Garda Síochána acting under the authority of a warrant to operate any computer at a place which is being searched,[2] and to require any person at that place, who has lawful access to the information in any such computer, to furnish any password necessary to operate it.

2. The applicant contends that this requirement and the offence created by any failure to comply with it, together with the consequential power of arrest, constitute a disproportionate interference with the privilege against self-incrimination.

3. The background to these proceedings concerns a complex investigation by the Serious Economic Crime Investigation Unit of the Garda National Economic Crime Bureau ("GNECB") in relation to suspected alleged criminal offences, including suspected

[1] The provisions which are sought to be impugned are sections 48(5)(b)(i), 49(1)(c) and 49(2) of the Criminal Justice (Theft and Fraud Offences) Act 2001. Section 48 was amended and substituted by section 192(1)(a) of the Criminal Justice Act 2006, subject to the transitional provisions in section 192(2) of that Act which provides that "[t]*his section shall not affect the validity of a warrant issued under section 48, or an order made under section 52, of the Criminal Justice (Theft and Fraud Offences) Act 2001 before the commencement of this section and such a warrant or order shall continue in force in accordance with its terms after such commencement.*"

[2] Or cause any such computer to be operated by a person accompanying the member for that purpose.

revenue offences, Companies Act offences, social welfare fraud and suspected offences of making gain or causing loss by deception, contrary to section 6 of the 2001 Act which arose consequent upon the conviction of Mr. Michael Lynn in December 2023.

4. As part of this ongoing garda investigation, on 8th January 2024, Detective Garda Laura Barton of the GNECB made an application to the District Court for a search warrant pursuant to section 48(2) of the 2001 Act to search the applicant's home address at Apartment 7, Saint Raphaela's Apartments, Saint Raphaela's Road, Kilmacud Road Upper, Stillorgan, County Dublin.

5. It was during the course of this search on 9th January 2024 that the Gardaí seized various items, including the following three devices: a Google Pixel 4 mobile smartphone, a Google Pixel 6 mobile smartphone and an Asus laptop.

6. The applicant confirmed that he owned these devices and that a password was required for each device.

7. When asked by the Gardaí for the passwords necessary to operate the devices, the applicant refused, which led to him being charged and prosecuted and, ultimately this application for judicial review in which leave was granted by this court (Hyland J.) on 15th April 2024 for an order of prohibition in relation to three charge sheets regarding the three devices and declaratory relief that section 48(5)(b)(i) (which conferred the power to require the applicant to provide the passwords), section 49(1)(c) (which creates the offence of failing to comply with this requirement) and section 49(2)

(which provides for the power of arrest in such circumstances) of the 2001 Act are respectively invalid having regard to the provisions of the Constitution.

8. Mark Lynam SC and Paul Comiskey O'Keefe BL appeared for the applicant. Kieran Kelly BL appeared on behalf of the Director of Public Prosecutions ("the DPP"). Remy Farrell SC and Joe Holt BL appeared on behalf of the Garda Commissioner, Ireland and the Attorney General ("the State respondents").

Statement of Grounds

9. Whilst the ultimate objective of this judicial review application (reflected in the prohibitory relief claimed) is to restrain the prosecution of the applicant on foot of Dundrum charge sheets numbers 25468486, 25468461 and 25468494 (in the context of the three devices) and notwithstanding the reference to the 'declaration of incompatibility' in section 5 of the European Convention on Human Rights Act 2003, in the Statement of Grounds, the gravamen of the applicant's challenge centred on his contention that the powers in sections 48 and 49 of the 2001 Act – which (i) confer the power to require the applicant to provide passwords for the three devices; (ii) create an offence when failing to comply with this requirement; and (iii) provide for a consequent power of arrest – are respectively invalid, having regard to the Constitution, in that it is claimed that they amount to a disproportionate interference with the applicant's asserted right to the privilege against self-incrimination.

10. While this is examined in more detail later in this judgment, these proceedings, therefore, come within that category of a judicial review application which seeks to challenge (in this case, part – but not all – of) the underlying legislative provisions in

section 48 of the 2001 Act which create an offence for failing to comply with a request to furnish a password in relation to computers.

11. In *Damache v DPP* [2012] IESC 11, [2012] 2 I.R. 266, at paragraph 12 of her judgment, Denham C.J. described this type of challenge, when dealing with the issue of prematurity in that case, as follows:

> "*This case is brought in advance of a trial. No evidence has yet been given. This is well illustrated by the grounding affidavit in these proceedings, deposed by the appellant's solicitor, based on a statement in the book of evidence of a member of An Garda Síochána. This is an unsatisfactory basis for analysis. However, the appellant has been affected by the section: his home was searched pursuant to a warrant issued under the section. This is not a case about the validity of the warrant. The sole issue is the constitutionality of s. 29(1) of the Act of 1939. In the circumstances the Court did not require to hear counsel on the issue of prematurity*".

12. The applicant's Statement of Grounds is dated 1st February 2024 and the facts referred to therein are set out in his Affidavit sworn on 1st February 2024. The applicant also exhibits a précis of the evidence proposed to be led by the prosecution at his summary criminal trial in an Affidavit sworn on 29th February 2024. The Notice of Motion is dated 17th April 2024.

Statement of Opposition

13. The State respondents' Statement of Opposition is dated 2nd July 2024 and is grounded and verified on the Affidavits of Detective Sergeant Wayne Donnelly sworn on 3rd July 2024, Detective Garda Anthony Woods sworn on 5th July 2024 and the Affidavit dated 9th July 2024 of Detective Sergeant Michael Ryan of the Garda National Cyber Crime Bureau addresses *inter alia* technical matters in relation to the Google Pixel 4 and 6 mobile smartphones. Mr. Michael Durkan, Senior Prosecutor in the Judicial Review Section of the Office of the DPP, swore a verifying Affidavit on 8th July 2024, insofar as the Statement of Opposition related to matters concerning the DPP.

THE STATUTORY PROVISIONS

Section 48 of the 2001 Act

14. Section 48 of the 2001 Act provides for '*search warrants*' as follows:

> "*48(1) This section applies to an offence under any provision of this Act for which a person of full age and capacity and not previously convicted may be punished by imprisonment for a term of five years or by a more severe penalty and to an attempt to commit any such offence.*
>
> ***(2) If a Judge of the District Court is satisfied by information on oath of a member of the Garda Síochána that there are reasonable grounds for suspecting that evidence of, or relating to the commission of, an offence to which this section applies is to be***

found in any place, the judge may issue a warrant for the search of that place and any person found there.

(3) A warrant under this section shall be expressed and shall operate to authorise a named member of the Garda Síochána, alone or accompanied by such other persons as may be necessary—

(a) to enter, within 7 days from the date of issuing of the warrant (if necessary by the use of reasonable force), the place named in the warrant,

(b) to search it and any persons found there,

(c) to examine, seize and retain any thing found there, or in the possession of a person present there at the time of the search, which the member reasonably believes to be evidence of or relating to the commission of an offence to which this section applies, and

(d) to take any other steps which may appear to the member to be necessary for preserving any such thing and preventing interference with it.

(4) The authority conferred by subsection (3)(c) to seize and retain any thing includes, in the case of a document or record, authority—

(a) to make and retain a copy of the document or record, and

(b) where necessary, to seize and, for as long as necessary, retain any computer or other storage medium in which any record is kept.

(5) A member of the Garda Síochána acting under the authority of a warrant under this section may—

(a) operate any computer at the place which is being searched or cause any such computer to be operated by a person accompanying the member for that purpose, and

(b) require any person at that place who appears to the member to have lawful access to the information in any such computer—

(i) to give to the member any password necessary to operate it,

(ii) otherwise to enable the member to examine the information accessible by the computer in a form in which the information is visible and legible, or

(iii) to produce the information in a form in which it can be removed and in which it is, or can be made, visible and legible.

(6) Where a member of the Garda Síochána has entered premises in the execution of a warrant issued under this section, he may seize and retain any material, other than items subject to legal privilege, which is likely to be of substantial value (whether by itself or together with other material) to the investigation for the purpose of which the warrant was issued.

(7) The power to issue a warrant under this section is in addition to and not in substitution for any other power to issue a warrant for the search of any place or person.

(8) In this section, unless the context otherwise requires—

"commission", in relation to an offence, includes an attempt to commit the offence;

"computer at the place which is being searched" includes any other computer, whether at that place or at any other place, which is lawfully accessible by means of that computer;

"place" includes a dwelling;

"thing" includes an instrument (within the meaning of Part 4), a copy of such instrument, a document or a record."[3]

15. Section 49 of the 2001 Act provides for the obstruction of a Garda acting on a warrant as follows:

"*49(1) A person who—*

(a) obstructs or attempts to obstruct a member of the Garda Síochána acting under the authority of a warrant issued under this Part, or

(b) is found in or at the place named in the warrant by a member of the Garda Síochána so acting and fails or refuses to give the member his or her name and address when required by the member to do so or gives the member a name and address that is false or misleading, or

(c) fails without lawful authority or excuse to comply with a requirement under paragraph (b) or section 48(5)(b),

[3] Emphasis added in this judgment.

is guilty of an offence and is liable on summary conviction to a fine not exceeding £500 or imprisonment for a term not exceeding 6 months or both.

(2) A member of the Garda Síochána may arrest without warrant any person who is committing an offence under this section or whom the member suspects, with reasonable cause, of having done so."

SWORN INFORMATION & SEARCH WARRANT

16. The application for the search warrant was grounded on a sworn Information for Search Warrant, sworn by Detective Garda Barton on 8th January 2024. The copy of the Sworn Information exhibited in this application for judicial review is extremely detailed and, due to the ongoing nature of the investigations, is also heavily redacted.

17. Insofar as the issues raised in this application for judicial review are concerned, the Sworn Information recites *inter alia* that Detective Garda Laura Barton had "*reasonable grounds for suspecting that*":

"evidence of, or relating to the commission of, an offence to which section 48 of the Criminal Justice (Theft and Fraud Offences) Act 2001 (as amended by section 192(1)(a) of the Criminal Justice Act 2006) applies is to be found in a place (within the meaning of section 48(8) of the Criminal Justice (Theft and Fraud Offences) Act 2001, namely Apartment 7, St Raphaela's Apartments, Saint Raphaela's

Road, Kilmacud Road Upper, Stillorgan, Co. Dublin in the said court (area and) district";

"*the nature of this criminal investigation involve breaches of the following:*

- *Section 6 of the Criminal Justice (Theft and Fraud Offences) Act 2001*
- *Section 251 of the Social Welfare Consolidation Act 2005*
- *Section 7 of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010*
- *Section 1078 of the Taxes Consolidation Act, 1997*";

"*Our investigations have found that there are reasonable grounds to believe suspect there are three companies which* [named persons] *have links to and/or access to their accounts … The first company is Ribblesway Limited which was established on the 4th May 2021. The current address for the company is* [address is set out]… *The company's current director is Yavor Todorov Poptoshev …"*

"*this part of the investigation … is focused on the belief that there is reasonable grounds to suspect that* [third party] … *is committing an offence under Section 6 of the Criminal Justice (Theft and Fraud Offences) Act 2001 insofar that* [they have] … *deceived the Department of Social Welfare … whilst this investigation believes* [they have] … *access to company accounts with substantial balances*

contained. The application for a warrant under these provisions is an operational one as a warrant under Section 48 of this Act allows for the requirement of the provision of passwords etc. on computers (which includes mobile phones). However as stated at the beginning of this information the investigation team suspect there are other offences being committed.

Gardai are satisfied that there is evidence relating to the offence under investigation to be found at [an address is set out]. *The said evidence includes but* [is] *not limited to:*

- *Financial documentation including bank documents, bank statements, payment cards, online login data;*
- *Identity documents;*
- *Cash, evidence of money transfers;*
- *Electronic devices including PCs, laptops, tablets, mobile phones, printers;*
- *Any other item(s) identified as being relevant to the investigation.*

The investigation team believes that evidence in relation to the aforementioned, can be found on electronic devices, mobile telephones, computers, servers, other electronic storage devices, etc. It is the intention of the investigation/search team to seek out these electronic devices and that if located, to seize and retain these items as evidence. It is also the intention of the investigation team to have

these electronic devices downloaded/copied/analysed/examined for digital evidence in relation to this investigation. This digital evidence will include seeking [sic.] *will be emails, social media connections, messages on messaging services, and any evidence on digital wallets.*

As a result of enquiries carried out by me into this investigation, I am satisfied that there is evidence of or relating to the commission of an offence under this act to be found at Apartment 7, St Raphaela's Apartments, Saint Raphaela's Road, Kilmacud Road Upper, Stillorgan, Co. Dublin.

I hereby apply for the issue of a warrant under section 48(2) of the Criminal Justice (Theft and Fraud Offences) Act 2001 (as substituted by section 192(1)(a) of the Criminal Justice Act 2006) in respect of that place and any person found at that place".

18. This application was granted by District Court Judge Shalom Binchy who issued a warrant, dated 8th January 2024, pursuant to section 48(2) of the 2001 Act in *inter alia* the following terms:

"*District Court Area of Dublin Metropolitan District*

WHEREAS from the information on oath and in writing under section 48(2) of the above mentioned Act of 2001(as substituted by section 192(1)(a) of the Criminal Justice Act 2006) sworn before me on this day, by Detective Garda Laura Barton of the Garda National Economic Crime Bureau, Clyde House, IDA Blanchardstown Business & Technology Park, Dublin 15.

A member of the Garda Síochána.

I AM SATISFIED THAT there are reasonable grounds for suspecting that –

evidence of, or relating to the commission of, an offence to which section 48 of the Criminal Justice (Theft and Fraud Offences) Act 2001(as amended by section 192(1)(a) of the Criminal Justice Act 2006) applies including but not limited to:-

- *Financial documentation including bank documents, bank statements, payment cards, online login data;*
- *Identity documents;*
- *Cash, evidence of money transfers;*
- *Electronic devices including PCs, laptops, tablets, mobile phones, printers ;*
- *Any other item(s) identified as being relevant to the investigation.*

AND any other items held by electronic means is to be found at a place, Apartment 7, St. Raphaela's Apartments, St. Raphaela's Road, Kilmacud Road Upper, Stillorgan, Co. Dublin, in the court (area and district) aforesaid.

THIS IS TO AUTHORISE Detective Garda Robert Tonkin of the Garda National Economic Crime Bureau, Clyde House, IDA Blanchardstown Business & Technology Park, Dublin 15, a member of the Garda Síochána accompanied by such other persons as the said member considers necessary.

TO ENTER at any time or times within seven days from the date of issuing of this warrant (if necessary by the use of reasonable force) the place, namely Apartment 7, St. Raphaela's Apartments, St. Raphaela's Road, Kilmacud Road Upper, Stillorgan, Co. Dublin in the said court (area and district) aforesaid.

TO SEARCH the said place and any persons found there.

TO EXAMINE, SEIZE and RETAIN anything found there, or in the possession of any person present there at the time of the search, which (s)he reasonably believes to be evidence of, or relating to the commission of, an offence to which section 48 of the said Act applies; and

TO TAKE any other steps which may appear to him/her to be necessary for preserving any such thing and preventing interference with it.

Dated this 8th day of January 2024

Signed Shalom Binchy[4]

Judge of the District Court

To:- Detective Garda Laura Barton of the Garda National Economic Crime Bureau".

Executing the search warrant

19. As set out earlier, the State respondents' Statement of Opposition is verified in a number of affidavits. Detective Sergeant Wayne Donnelly of the GNECB was a member of the search team which executed the search warrant at the premises on 9th January 2024. The applicant was present when the Gardaí arrived at the premises. The warrant holder, Detective Garda Robert Tonkin of the GNECB, showed a copy of the warrant to the applicant and explained its provisions to him. In his verifying affidavit sworn on 3rd July 2024, Detective Sergeant Donnelly confirmed that he identified himself to the applicant and explained that the search warrant that he had been shown allowed Detective Sergeant Donnelly to enter and search his property and to take away any items which he believed were relevant to the investigation. Detective Sergeant Donnelly sets out in his affidavit that the applicant indicated to him that he understood and added at paragraph 21 of his Affidavit that:

"*I then cautioned the Applicant in the usual terms by stating "You are not obliged to say anything unless you wish to do so but anything you do say will be taken down in writing and may be given in evidence." I asked him if he understood the caution and he asked me if I could*

[4] The signature of Judge Shalom Binchy is set out in the exhibited Search Warrant.

repeat it, which I did. I then explained to him in ordinary language what the caution meant. The Applicant told me that he understood".

20. On a number of occasions during the search, the applicant asked if he could read the warrant and was facilitated in doing so on each occasion.

21. During the search, members of An Garda Síochána seized various items, including hardcopy documentation and electronic devices.

22. Insofar as the discrete issue raised in this application for judicial review is concerned, among the items seized during the search were the following three devices: a Google Pixel 4 mobile smartphone; a Google Pixel 6 mobile smartphone; and an Asus laptop.

23. When asked by Detective Sergeant Donnelly, the applicant confirmed that he owned the three devices and that a PIN number or password was required for each device. Detective Sergeant Donnelly, having considered that the applicant had lawful access to the information on each device, requested the applicant, pursuant to section 48(5)(b)(i) of the 2001 Act, to give him any password necessary to operate the devices.

24. Detective Sergeant Donnelly showed the applicant the provisions of section 48(5) of the 2001 Act by accessing the legislation on *irishstatutebook.ie* on his mobile phone, and he also explained the provisions of section 48(5) of the 2001 Act to the applicant in ordinary language. It was further explained to the applicant that a failure to comply with the request constituted a criminal offence for which he could be arrested.

25. The applicant requested to speak to a solicitor. Detective Sergeant Donnelly rang the applicant's nominated solicitor but there was no answer and Detective Sergeant Donnelly left a message asking him to return the call.

26. Detective Garda Anthony Woods of the GNECB then asked the applicant again, pursuant to section 48(5)(b)(i) of the 2001 Act, to give him any password necessary to operate the said devices. The applicant was again informed of the consequences of a failure to comply with the lawful requirement made of him to provide the passwords for the devices in question. The applicant refused to provide the passwords or PIN numbers for either of the two mobile smartphones or the laptop.

27. Consequent upon the applicant's refusal to provide the passwords or PIN numbers for the Google Pixel 4 mobile smartphone, the Google Pixel 6 mobile smartphone and the Asus laptop, he was arrested by Detective Garda Woods pursuant to section 49(2) of the 2001 Act for an offence contrary to section 49(1)(c) of the 2001 Act, namely his failure without lawful authority or excuse to comply with a requirement made of him under section 48(5)(b) of the 2001 Act.

28. The applicant was then brought to Dundrum Garda Station and, after having been processed, the applicant had three telephone consultations with his solicitor at 10:05am, 10:37am and, 11:02am.

29. Detective Garda Woods spoke to the applicant's solicitor over the telephone and told him that the applicant was detained and awaiting being charged. Detective Garda

Woods explained the reasons for this to the applicant's solicitor. The applicant's solicitor subsequently telephoned back to say that having consulted with counsel, it was his advice that section 48 of the 2001 Act did not apply to the mobile phones. Detective Garda Woods then explained the requirements of the legislation. The applicant's solicitor stated that the applicant was willing to provide the passwords if An Garda Síochána gave an undertaking not to search the devices until the method and parameters of the search had been agreed. Detective Garda Woods said that this was not his decision to make.

30. The applicant then had a further telephone conversation with his solicitor. Thereafter, he explained to An Garda Síochána that he had received legal advice to the effect that the power to acquire the production of a password did not apply to mobile phones and that he was not obliged to provide his password. As regards his laptop, the applicant said that a date could be arranged for An Garda Síochána to examine it in his presence.

31. Given that the applicant was refusing to provide the requested passwords, he was informed that he was to be charged and he was subsequently charged with three offences – "*that on 9th January 2024 at Apartment 7, Saint Raphaela's Apartments, Saint Raphaela's Road, Kilmacud Road Upper, Stillorgan, Dublin in the District Court Area of Dublin Metropolitan District, being a person having lawful access to information on a computer did fail, without lawful authority or excuse to comply with a requirement made by Detective Garda Anthony Woods under section 48(5)(b) of the Criminal Justice (Theft and Fraud Offences) Act, 2001 in that [the applicant] did (i) fail to give Detective Garda Anthony Woods any password necessary to operate a*

computer, namely [a Google Pixel 4 mobile phone], [a Google Pixel 6 mobile phone], [an Asus laptop], Contrary to section 49(1)(c) of the Criminal Justice (Theft and Fraud Offences) Act 2001."

32. By letter dated 9th February 2024, the applicant was provided with a schedule of the items seized from his apartment and invited to identify the materials over which he was claiming legal professional privilege and the reasons for same. The applicant's solicitor responded by letter dated 25th April 2024 seeking an inspection of the relevant materials prior to particularising his claim of privilege.

33. The Chief State Solicitors' Office sent a letter to the applicant's solicitor dated 18th June 2024 inviting the applicant to confirm on whose behalf he was claiming legal professional privilege over the exhibits seized from the apartment. The letter outlined that if the applicant was claiming legal professional privilege on his own behalf, he was invited to identify the nature of the legally privileged relationship in question and describe the basis for such claim of privilege. No response to that letter was received.

34. The applicant applied for leave to apply for judicial review and same was granted by Order of this Court (Hyland J) on 15th April 2024.

Evidence of Detective Sergeant Michael Ryan

35. As mentioned earlier, Detective Sergeant Michael Ryan is a member of the Garda National Cyber Crime Bureau in charge of its cyber investigations unit.

36. He is a holder of a First-Class Honours Masters' Degree in Computer Forensics and Cybercrime Investigation from University College Dublin. He is a trained and certified operator of the XRY Logical Mobile Phone Forensic Examination software and equipment by MicroSystemation.

37. Detective Sergeant Ryan is a trained and certified operator of the XRY physical (XACT) advanced mobile phone forensic examination equipment and software by MicroSystem. He is also a trained and certified operator of the UFED Complete (Universal Forensic Extraction Device) mobile phone device forensic examination equipment and software by Cellebrite. He is a member of the International Association of Computer Investigative Specialists (IACIS) and completed the IACIS certified mobile device examiner's (ICMDE) certification process. He is also trained and certified as a Magnet Axiom Forensic Examiner (MCFE). Magnet Axiom is a digital investigation platform that enables the forensic extraction and analysis of digital evidence from a wide range of digital devices, including computers and mobile telephone devices. Detective Sergeant Ryan completed training with Belkasoft in Android Forensics and is certified in respect of the use of this toolset for the analysis of such devices.

38. He has also completed certified training in the use of Autopsy by Basis Technology, which is a digital forensics platform used for conducting in-depth examinations of digital devices and file systems; he is trained in the use of the Graykey mobile telephone device extraction tool. Detective Sergeant Ryan has also completed a dedicated training course on the electronic analysis of telephone account data and

successfully completed the telephone liaison officer's course within An Garda Síochána.

DISCUSSION & DECISION

Existence of material independent of the will of the applicant

39. The privilege against self-incrimination is not engaged by the use in criminal proceedings of material obtained from an accused through compulsory powers but which has an existence independent of the will of the accused or suspect.

40. In *R v S (F)* [2009] 1 WLR 1489 (judgment delivered by Lord Judge C.J., with Penry-Davey and Simon JJ) Lord Judge C.J. observed (at paragraph F,18, p. 1495) that the first question which arises in an individual case is not in relation to the statutory exceptions to the principle against self-incrimination but whether or not the principle is in fact engaged. For the following reasons, I am of the view that the privilege against self-incrimination is not in fact engaged in this case.

41. In *Saunders v UK* (Application No. 19187/91), the ECtHR referred *inter alia* at paragraph 68 to "[t]*he right not to incriminate oneself, in particular, presupposes that the prosecution in a criminal case seek to prove their case against the accused without resort to evidence obtained through methods of coercion or oppression in defiance of the will of the accused*" and at paragraph 69, "[t]*he right not to incriminate oneself is primarily concerned, however, with respecting* ***the will of an accused person to remain silent****. As commonly understood in the legal systems of the Contracting Parties to the Convention and elsewhere****, it does not extend to the use in***

criminal proceedings of material which may be obtained from the accused through the use of compulsory powers but which has an existence independent of the will of the suspect such as, inter alia, documents acquired pursuant to a warrant, breath, blood and urine samples and bodily tissue for the purpose of DNA testing." [Emphasis and underlining added in this judgment].

42. After quoting the above paragraph 69 from *Saunders*, Clarke J. (as he then was) observed in joint cases, *DPP v Gormley*; *DPP v White* [2014] IESC 17 at paragraph 6.8 of his judgment that "[t]*his principle, that the privilege against self-incrimination does not apply to blood or other physical or objective specimens used in forensic analysis, was recently reaffirmed in Boyce v Ireland (Application 8428/09 (Fifth Section), 12th November, 2012), a case concerning the taking of a blood sample.*"

43. The Supreme Court made similar *obiter* comments in *Curtin v Dáil Éireann* [2006] 2 I.R. 556, relying again on the passage at paragraph 69 from the judgment of the ECtHR in *Saunders* observing that "*it is appropriate to draw attention to the distinction between a requirement that a person make a statement or give evidence which may tend to incriminate him and a requirement that a person produce for inspection, whether by An Garda Síochána or other organs of the State, a physical article, including a document … The last type of power may require the owner of the dwelling house to permit the search to take place and cooperate with the gardaí in finding materials to take away. It cannot be said that this type of power involves any element of self-incrimination. This distinction is well described in the important decision of the European Court of Human Rights in the case of Saunders v UK … at paragraph 69*".

44. The decision of the Court of Appeal in England in *R v S (F)* [2009] 1 WLR 1489 referred to a number of cases including the decision of the ECtHR in *Saunders v UK* (1996) 23 EHRR 313, and the reported judgment confirms that the following decisions were referred to in skeleton arguments: *Funke v France* (1993) 16 EHRR 297; *Heaney & McGuinness v Ireland* (2000) 33 EHRR 264; *JB v Switzerland* [2001] Crim LR 748.

45. I would not, therefore, agree with the argument made on behalf of the applicant that there is any confusion arising from the decision of the ECtHR in *Saunders v UK*. In addition to its endorsement in the interpretation of the privilege against incrimination in Irish and UK case law (as set out in this judgment), it remains the central authority and explanation relied upon by the ECtHR as illustrated in the following observations of the Strasbourg Court in *De Legé v The Netherlands* (Application no. 58342/15) (4th October 2022) at paragraph 67:

> "*(67) The right not to incriminate oneself is primarily concerned, however, with respecting the will of an accused person to remain silent. As commonly understood in the legal systems of the Contracting Parties to the Convention and elsewhere, it does not extend to the use in criminal proceedings of material which may be obtained from the accused through the use of compulsory powers but which has an existence independent of the will of the suspect such as, inter alia, documents acquired pursuant to a warrant, breath, blood and urine samples and bodily tissue for the purpose of DNA testing (see Saunders, cited above, § 69; Kalnėnienė v. Belgium,*

no. 40233/07, § 52, 31 January 2017; Sršen v. Croatia (dec.), no. 30305/13, § 44, 22 January 2019; and El Khalloufi v. the Netherlands (dec.), no. 37164/17, §§ 38-40, 26 November 2019). However, where such evidence has been obtained by a measure which breaches Article 3, the privilege against self-incrimination remains applicable (see also Jalloh, cited above, §§ 105, 108 and 115-16)".

46. In addition, the judgments in *De Legé v The Netherlands* (Application no. 58342/15) (4th October 2022), *Funke v France* (1993) 16 EHRR 297, *JB v Switzerland* ECtHR, (Application No. 31827/96, 3rd May 2001), and *Chambaz v Switzerland* (App. No.11663/04) upon which reliance was placed on behalf of the applicant, related to *production orders* in respect of documents including, for example, the production of financial documentation in relation to tax, revenue and customs matters (rather than search warrants) which the authorities suspected existed but were not certain, which raises the privilege against self-incrimination in a similar way to the US case law dealing with the forgone conclusion doctrine and production doctrine, *i.e.*, the action of production becomes a form of implied assertion. This is different to the situation in this challenge where the Google Pixel 4 mobile smartphone, Google Pixel 6 mobile smartphone and the Asus laptop were lawfully seized by the Gardaí under a warrant issued by the District Court on foot of a Sworn Information and they seek the "*key*" or password as described by Lord Judge CJ in *R v S (F)* [2009] 1 WLR 1489 at paragraph 20 (and referred to later in this judgment).

47. In terms of statutory exceptions to the common law rule, in *R v S (F)* [2009] 1 WLR 1489 from 1494 to 1495 (beginning at paragraph 17, H), Lord Judge C.J. stated as follows:

> "*It is well understood that the principle is subject to numerous statutory exceptions which limit, amend, or abrogate the privilege in specified circumstances. Thus, notwithstanding the privilege, individuals may sometimes be required to answer questions or provide information or documents which may incriminate them. As Lord Mustill explained in R v Director of Serious Fraud Office, ex p. Smith [1993] AC 1, 31 in relation to the general immunity against answering incriminating questions, "…few would dispute that some curtailment of the liberty is indispensable to the stability of society; and indeed in the United Kingdom today our lives are permeated by enforceable duties to provide information on demand'*"".

48. Lord Judge C.J. also referred to *Browne v Stott* [2003] 1 AC 681, at p. 704, where Lord Bingham had explained the effect of the jurisprudence of the ECtHR as follows:

> "*that while the overall fairness of a criminal trial cannot be compromised, the constituent rights comprised, while expressly or implicitly, within Article 6 are not themselves absolute. Limited qualification of these rights is acceptable if reasonably directed by national authorities towards a clear and proper public objective and if representing no greater qualification than the situation calls for*".

49. In *R v S (F)* [2009] 1 WLR 1489 at p.1498 (paragraphs 24, A to D and paragraphs 25 E to H) the court set out that the correct analysis was that the privilege against self-incrimination "*may*" be engaged by a requirement of disclosure of knowledge of the means of access to protected data under compulsion of law, stating that:

> "*although the defendants' knowledge of the means of access to the data may engage the privilege against self-incrimination, it would only do so if the data itself–which undoubtedly exists independently of the will of the defendants and to which the privilege against self-incrimination does not apply – contains incriminating material. If the data was neutral or innocent, the knowledge of the means of access to it would similarly be either neutral or innocent. On the other hand, if the material were, as we have assumed, incriminatory, it would be open to the trial judge to exclude the evidence of the means by which the prosecution gained access to it. Accordingly the extent to which the privilege against self-incrimination may be engaged is indeed very limited*".

50. The appropriate forum to adjudicate the interpretation of any criminal offence and the admissibility of any evidence (including that just described) in support of it, is the *court of trial*. Within that forum, the trial judge has the advantage of access to the entirety of the book of evidence and may also call for any other statement or correspondence that is relevant to such adjudication: *Sweeney v Ireland* [2019] IESC 39 per Charleton J. at paragraph 3.

51. Whilst also referred to later in this judgment, the decision of the High Court (Kearns J., as he then was) in *Dunnes Stores Ireland Company v Ryan* [2002] 2 I.R. 60 addressed the question as to whether the right to silence and the privilege against self-incrimination were contravened by the provisions of sections 19(5) and 19(6) of the Companies Act 1990, and if so, whether this infringed the provisions of the Constitution dealing with the right to silence.

52. Section 19(5) of the Companies Act 1990 provided:

> "*If a requirement to produce books or documents or provide an explanation or make a statement which is imposed by virtue of this section is not complied with, the body or other person on whom the requirement was so imposed shall be guilty of an offence; but where a person is charged with an offence under this subsection in respect of a requirement to produce any books or documents, it shall be a defence to prove that they were not in his possession or under his control and that it was not reasonably practicable for him to comply with the requirement.*"

53. Section 19(6) of the Companies Act 1990 provided:

> "*A statement made by a person in compliance with a requirement imposed by virtue of this section may be used in evidence against him.*"

54. Beginning at paragraph 83 of his judgment in *Dunnes Stores Ireland Company v Ryan*, Kearns J. referred to the narrow objective of section 19 of the Companies Act

1990 being to obtain sight of books and documents with a view to seeing if an inspector should be sent in to examine the company's affairs under another section, and that the Court must also take into account that where the incriminating material has "*an objective reality*" the requirement for protection is less compelling.

55. The court referred to the following observations of Sachs J. in *Ferreira v Levin and Others* 1996 (1) BCLR 1 (CC) at p. 274, "*the more that self-incrimination takes the form of oral communication, the more compelling will the protection be; the more objective or real the existence of the incriminating material, on the other hand, the more attenuated. Accordingly, pre-trial procedures of a non-communicative or non-testimonial kind, such as compulsory fingerprinting, blood tests, blood alcohol tests, attendance at identity parades, DNA and other tests of an objective nature, or, in company fraud matters, hand writing tests, all of which would seem to fall directly under the concept of freedom and personal security, have become well established processes regarded in many parts of the world as being consistent with the values of an open and democratic society based on freedom and equality, and in suitably controlled conditions, would have far less difficulties in passing Section 33 scrutiny in terms of our Constitution*".

56. Further, Kearns J. observed that this consideration was also acknowledged by the ECtHR in *Quinn v Ireland* (ECHR 21.3.2001) where the court observed at p. 12 that "[t]*he right not to incriminate oneself is primarily concerned, however, with respecting the will of an accused person to remain silent. The Court would note, in this context, that the present case does not concern a request, through the use of*

compulsory powers, of material which had an existence independent of the will of the applicants such as, documents or blood samples."

57. In *R v Kearns* [2002] 1 WLR 2815, at paragraph 53 Aikens J. had also observed that:

> "*There is a distinction between the compulsory production of documents or other material which have an existence independent of the will of the suspect or accused person and statements that he has had to make under compulsion. In the former case there is no infringement of the right to silence and the right not to incriminate oneself. In a lot of cases there could be, depending on the circumstances.*"

58. In *R v S (F)* [2009] 1 WLR 1489 at p. 1496 (paragraphs 19, C and 20 D to E) Lord Judge C.J. observed as follows:

> "*19. These authorities, and many of the other authorities cited to us, meant that the debated argument concentrated on the rival contentions whether the key to each defendant's protected data was properly to be catalogued as a piece of information with an existence separate from his "will". The problem which presents itself in the present appeals, is not, in our judgment, susceptible of quite such rigid compartmentalisation.*
>
> *20. On analysis, the key which provides access to protected data, like the data itself exists separately from each defendant's "will'. Even if it is true that each created his own key, once created the key to data was independent of the defendant's "will" even when it is retained only in*

his memory, at any rate until it is changed. If investigating officers were able to identify the key from a different source (say, for example from the records of the shop where the equipment was purchased) no one would argue that the key was not distinct from the equipment which was to be accessed, and indeed the individual who owned the equipment and knew the key to it. Again, if the arresting officers had arrived at the premises in Sheffield immediately after S had completed the process of accessing his own equipment enabling them to identify the key, the key itself would have been a piece of information existing, at this point, independently of S himself and would have been immediately available to the police for their use in the investigation. ***In this sense the key to the computer equipment is no different from the key to a locked drawer. The contents of the drawer exist independently of the suspect: so does the key to it. The contents may or may not be incriminating: the key is neutral***".[5]

59. During the course of giving effect to the search warrant the evidence is (as set out above) that the Gardaí explained each step of the process to the applicant.

60. To recap, by way of summary, Detective Garda Robert Tonkin showed a copy of the warrant to the applicant and explained its provisions to him. Detective Sergeant Donnelly explained that the search warrant which he had shown to the applicant allowed him to enter and search his property and to take away any items which he believed were relevant to the investigation and the applicant indicated to him that he

[5] Emphasis added in this judgment.

understood. The applicant was cautioned in the usual terms. It was repeated and explained in ordinary language which the applicant confirmed he understood. On a number of occasions, during the search, the applicant asked if he could read the warrant and was facilitated in doing so on each occasion.

61. During the search, a Google Pixel 4 mobile smartphone, a Google Pixel 6 mobile smartphone and an Asus laptop, which the applicant confirmed he owned and that passwords were required for each device, were seized. Detective Sergeant Donnelly, having considered that the applicant had lawful access to the information on each device requested the applicant, pursuant to section 48(5)(b)(i) of the 2001 Act, to give him any password necessary to operate the devices. The provisions of section 48(5) of the 2001 Act were shown to the applicant by Detective Sergeant Donnelly by accessing the legislation on *irishstatutebook.ie* on his mobile phone and explained to the applicant in ordinary language.

62. It was further explained to the applicant that a failure to comply with the request constituted a criminal offence for which he could be arrested. The applicant requested to speak to a solicitor. Detective Sergeant Donnelly rang the applicant's nominated solicitor but there was no answer and Detective Sergeant Donnelly left a message asking him to return the call. Detective Garda Anthony Woods asked the applicant again, pursuant to section 48(5)(b)(i) of the 2001 Act, to give him any password necessary to operate the said devices. The applicant was again informed of the consequences of a failure to comply with the lawful requirement made of him to provide the passwords for the devices in question. The applicant refused to provide the passwords and thereafter he was arrested by Detective Garda Woods pursuant to

section 49(2) of the 2001 Act for an offence contrary to section 49(1)(c) of the 2001 Act, namely his failure without lawful authority or excuse to comply with a requirement made of him under section 48(5)(b) of the 2001 Act.

63. I consider, therefore, that the provisions in section 48(5)(b)(i) of the 2001 Act, which, on the facts of this case conferred the power on the Gardaí to require the applicant to provide passwords for the three devices, come within the analysis of Lord Judge C.J. (by way of example, at paragraph 20 of his judgment in *R v S (F)* [2009] 1 WLR 1489) and that the passwords in relation to the Google Pixel 4 mobile smartphone, the Google Pixel 6 mobile smartphone and the Asus laptop, constituted 'keys' which provided access to information on the three devices, and as with that information, the passwords existed separately from the applicant's "*will*" so that if the applicant, in this case, created his own key (or passwords), once created the keys (or passwords) to that information were independent of the applicant's "*will*" "*even when they are retained only in his memory, at any rate until they are changed*." The existence of the passwords in this case in relation to the two mobile phones (and the laptop), in my view, exist *independent of the will* of the applicant.

64. In addition, I note the following commentary, which echoes the analysis of Lord Judge CJ in *R v S (F)* [2009] 1 WLR 1489, in the UK Home Office paper "Investigation of Protected Electronic Information" (Revised Code of Practice (August 2018) under the sub-heading, "Description of a key", at paragraphs 3.18 and 3.19:

"*3.18 A key to data means any key, code, password, algorithm or other data (including any proprietary software or cryptographic process) the use of which, by itself or with another key or keys:*

- *allows protected electronic data to be accessed, or*
- *facilitates putting protected electronic data into an intelligible form.*

3.19 All manner of material can constitute a key. A key can be a plain language password or pass-phrase. It can include, for example, words, phrases or numbers written on any form of paper, plastic cards bearing numbers, electronic chips or magnetic strips and all forms of removable or fixed media for storing electronic data. It can include intangible material, for example, sounds or movements or comprise biometric data derived from, for example, fingerprint readers or iris scanners. Equally key material can be retained in the memory of an individual".

65. During the course of the hearing, I was referred to proceedings entitled *Minteh v France* (23624/20) which status, at the time of the delivery of this judgment, remains that of a case '*communicated*' to the ECtHR and, therefore, while of general interest, I place no reliance on. It relates to the provision of an offence under Article 434-15-2 of the French criminal code in the circumstances of where an individual having knowledge of the decryption procedure for access to an encrypted device that could have been used to prepare, facilitate or commit a serious offence, refuses to disclose that procedure to the judicial authorities or to use it when so directed by the authorities. In that case, the applicant was charged and sentenced pursuant to Article

434-15-2 of the French Criminal Code for refusing to communicate to French police officers the access code to his mobile telephone to police officers while in police custody. In his complaint to the Strasbourg Court, the applicant complains that this was a breach of his right to remain silent and not to incriminate himself together with a breach of his right to respect for his private life and for his correspondence.

Constitutional issue

66. In *DPP v Wilson* [2017] IESC 53, the Supreme Court (McKechnie J.) observed that both the right to silence and the privilege against self-incrimination are "*common law and constitutional aspects of the same coin*" and he referred to *Re National Irish Bank Limited (No.1)* [1999] 3 I.R. 145 at page 173 for a judicial perspective on the historical development of the right, and further referenced *Heaney & Anor v Ireland & Anor* [1996] 1 I.R. 580, observing that its status at constitutional level was expressly acknowledged by both the High Court and the Supreme Court.

67. In *Heaney*, the High Court (Costello J., as he then was) considered that the privilege against self-incrimination was to be found in Article 38.1, whilst the Supreme Court expressly reserved its view on that question, preferring instead, in the context of that case, to describe the right as being a "*corollary*" to the freedom of expression provision in Article 40.6 of the Constitution. In *Re National Irish Bank Limited (No.1)* [1999] 3 I.R. 145, the Supreme Court affirmed that the general right to silence was derived from the right to freedom of expression guaranteed to citizens by Article 40.6 of the Constitution.

68. Insofar as the applicant's constitutional challenge is concerned, I consider, for the following reasons, that section 48(5)(b)(i) of the 2001 Act (which confers the power to require the applicant to provide passwords for the three devices), section 49(1)(c) of the 2001 Act (which creates an offence when failing to comply with this requirement), and section 49(2) of the 2001 Act (which provides for the power of arrest) are: (i) rationally connected to the objective of a member of An Garda Síochána acting under the authority of a warrant issued under section 48 to operate any computer at the place which is being searched (or cause any such computer to be operated by a person accompanying the member for that purpose) and is objective, not arbitrary, unfair or based on irrational considerations; (ii) impacts the right to freedom of expression or the provisions of Article 38.1 as little as possible; and (iii) is such that its effects on such rights are proportional to the objective sought: *Heaney v Ireland* [1994] 3 I.R. 593 per Costello J. (also referring *inter alia* to *Chaulk v* R [1990] 3 S.C.R. 1303, pp. 1335 and 1336.)

69. Section 48(5)(b)(i) (and in consequence section 49(1)(c) and section 49(2)) of the 2001 Act (being a post-1937 legislation) enjoy the *presumption of constitutionality* and are proportionate in addressing the provision of passwords in relation to the smartphones and the laptop at issue and in the circumstances of this case, as outlined above. In *Sweeney v Ireland* [2019] IESC 39 (at paragraph 72), Charleton J. referred to the presumption of constitutionality and the double-construction rule, in stating that it is presumed that all legislation passed since 1937 is in conformity with the Constitution and that where two possible constructions are open in interpreting legislation, it was the court's duty not to strike down legislation through adopting an unconstitutional construction; rather, the interpretation consistent with the

Constitution should be given where this is open. He referenced *McDonald v Bord na gCon* [1965] I.R. 217, having earlier referred to the observations of O'Donnell J. (as he then was) in *Jordan v Minister for Children and Youth Affairs* [2015] 4 I.R. 232 at paragraph 199, that a court must always "[a]*ddress the effect of the double construction rule and consider if the Constitution requires that the interpretation advanced by the petitioner while less likely, should nevertheless be accepted because the more likely interpretation of the words to require a showing of material effect, would be unconstitutional.*" Charleton J. added that it was also to be presumed that powers of administration conferred by legislation will be applied in a constitutional manner: *East Donegal Cooperative v Attorney General* [1970] 1 I.R. 317.

70. The precise terms of the provisions which are sought to be impugned are important: section 48(5)(b)(i) of the 2001 Act provides, for example, that a member of An Garda Síochána acting under the authority of a warrant under section 48 may require any person at that place who appears to the member to have lawful access to the information in any such computer to give to the member any password necessary to operate it; section 49(1)(c) of the 2001 Act provides that a person who fails without lawful authority or excise to comply with a requirement under section 49 (b) or section 48(5)(b) (which is the provision at issue in this case) is guilty of an offence and is liable on summary conviction to a fine not exceeding £500 or imprisonment for a term not exceeding 6 months or both; section 49(2) of the 2001 Act provides that a member of An Garda Síochána may arrest without warrant any person who is committing an offence under this section or whom the member suspects, with reasonable cause, of having done so. Furthermore, the applicant accepts that he owns

the two smartphones (a Google Pixel 4 and a Google Pixel 6) and the Asus laptop, found during the search.

71. During the course of this search of his dwelling on 9th January 2024, the applicant refused to accede to a direction by the gardaí to provide passwords for the two smartphones (a Google Pixel 4 and a Google Pixel 6) and the Asus laptop seized and he was subsequently charged. The gravamen of the applicant's challenge is that the invocation of these provisions – section 48(5)(b)(i), section 49(1)(c) and section 49(2) of the 2001 Act – by the gardaí, in the circumstances of this case, amounted to a disproportionate interference with the privilege against self-incrimination and as a consequence his trial should be prohibited.

72. Section 48 of the 2001 Act was the Oireachtas's response to the process of encryption. In addition to there being no ('administrative law') challenge to the actual warrant which was issued and executed in this case, there is also no challenge to the underlying provisions in section 48(3) of the 2001 Act (providing *inter alia* the power to enter, search, examine, seize, retain, preserve and prevent interference) or section 48(4) of the 2001 Act, which includes the power to seize and, for as long as necessary, retain any computer or other storage medium in which any record is kept. As the applicant has not sought to quash the warrant issued by the District Court on 8th January 2024 it enjoys the *presumption of validity* which attaches to public acts generally and is necessary in the interests of good order and administration: *In re Comhaltas Ceoltóirí Éireann* (Unreported, High Court, Finlay P., 5th December, 1977), *Campus Oil Ltd v Minister for Industry and Energy (No. 2)* [1983] I.R. 88, *The State (Divito) v Arklow Urban District Council* [1986] ILRM 123, *Ramaabya & Ors v*

The Minister for Justice & Equality [2020] IEHC 283; see also Mark De Blacam SC, *Judicial Review*, (3rd Edition, Dublin, Bloomsbury 2017) at p. 147.

73. The Google Pixel 4 and Google Pixel 6 smartphones and the Asus laptop are, therefore, lawfully in the hands of the Gardaí. To paraphrase Lord Judge C.J. in *R v S (F)* [2009] 1 WLR 1489 at p. 1498 (at paragraph 25 E to H), "[i]*n these appeals the question which arises, if the privilege is engaged at all, is whether the interference with it is proportionate and permissible. A number of issues are clear and stark. The material which really matters is lawfully in the hands of the police. Without the key it is unreadable. That is all. The process of making it readable should not alter it other than putting it into an unencrypted and intelligible form that it was in prior to encryption; the material in the possession of the police will simply be revealed for what it is. To enable the otherwise unreadable to be read is a legitimate objective which deals with a recognised problem of encryption*". As mentioned earlier, in addition there also exists the facility of the trial judge dealing with this and other issues by way appropriate rulings and directions.

74. In *Dunnes Stores Ireland Company v Ryan* [2002] 2 I.R. 60, Kearns J., (as he then was) applied the proportionality test in *Heaney v Ireland* [1996] 1 I.R. 580 (SC) ([1994] 3 I.R. 593 (HC)) to a constitutional challenge to sections 19(5) and 19(6) of the Companies Act 1990 with diverging results: section 19(5) was held to be constitutional whereas section 19(6) was held to be unconstitutional and set out at [2002] 2 I.R. 60, pp. 119 and 123:

> "(p.119) … *Taking all these considerations into account, I am satisfied that s.19(5) does not fail the proportionality test indicated by*

the Supreme Court in Heaney v Ireland [1996] 1 I.R. 580. The compulsion to produce books and documents is completely unobjectionable and the requirement to answer questions of fairly limited nature under section 19 does not in my view, constitute an infringement of Article 40 of the Constitution of sufficient substance to warrant condemning the section when weighed in the balance with the countervailing public interest in good corporate governance.

There is, at the end of the day, a world of difference between the position of a vulnerable suspect, held in police custody, say for example, for the investigation of a domestic homicide and that of a large corporation which may engage in all sorts of stratagems and then call on vast financial resources and expertise to protect and defend its position to the ultimate. I am not here referring to the present applicants, but rather contrasting by example the hugely different contexts in which the right to silence must be considered.

The real difficulty, it seems to me, lies in s.19(6). The examinee is obliged, on pain of punishment for a refusal, to answer questions or provide explanations which may be incriminating and which may be used in subsequent criminal proceedings against him …

(p.123) … I find that s.19(6), by not immunising answers given from later use in criminal proceedings, (and to that extent only) infringes the "minimum invasion" test enunciated by Costello J. in Heaney v Ireland…I am somewhat fortified in reaching this conclusion by the knowledge that the new amending legislation has provided for just

such an "immunisation" clause, although I could not and have not allowed that determine my own views on the matter which I have arrived at for the reasons stated".

75. Insofar as the applicant in this case also seeks to argue that a similar failure to immunise answers applies to section 48(5)(b)(i) of the 2001 Act, as I have already set out, the positions are not analogous. The search warrant and the sworn Information in this case issued under section 48 of the 2001 Act and contained detailed particulars of the alleged offences which also informed the District Judge, who issued the warrant, that the search may include *inter alia* digital and electronic devices, such as computers (including mobile phones). Ultimately, the privilege against self-incrimination was not engaged in this case: (as set out later in this judgment) the Google Pixel 4 mobile smartphone, the Google Pixel 6 mobile smartphone and the Asus laptop were all computers as provided for in section 48 of the 2001 Act where the existence of the passwords in relation to each of these three devices existed independent of the will of the applicant.

76. Borrowing, by way of analogy, the observations of Charleton J. at paragraphs 33 and 67 of the judgment of the Supreme Court in *Sweeney v Ireland* [2019] IESC 39, I consider that section 48(5)(b)(i) of the 2001 Act (which confers the power to require the applicant to provide passwords for the three devices), section 49(1)(c) of the 2001 Act (which creates an offence when failing to comply with this requirement), and 49(2) of the 2001 Act (which provides for the power of arrest) together require the cooperation of the applicant in circumstances which constitute a proportionate response to the investigation of suspected serious offences and are an attempt to

achieve proportion and balance in the context of the community's entitlement to investigate crime.

77. In addition, there are, I believe, some limitations in relying on diverse international case law with their respective distinct constitutional and legislative architecture when assessing a challenge such as this one in this judicial review application.

78. In my view, the Irish constitutional and common law position in the authorities examined is consistent with that outlined in the Strasbourg Court jurisprudence (*Saunders*) and the UK case law, such as the analysis carried out by Lord Judge C.J. in *R v S (F)* [2009] 1 WLR 1489, than the US, Canadian and Australian authorities cited.

79. In assessing, for example, the US 'active production' and 'foregone conclusion' doctrines, the Fifth Amendment to the Constitution of the United States or 'compelled production orders' in Australia and Canada, including, for example, the decision of the Court of Appeal in Quebec in *R v Boudreau-Fontaine* [2010] QCCA 1108, the following observations by Daniel Hochstrasser Lecturer, Graduate School of Business and Law, RMIT University, in a paper entitled "*Encryption and Privilege against self-Incrimination: what happens when a suspect refuses to divulge a password*",[6] (and contained in the Book of Authorities prepared for this hearing) are of assistance:

> "*What is retrieved from the encrypted device is pre-existing evidence of the type that has, until the widespread availability of encryption,*

[6] [2022] UNSWLawJl 37; (2022) 45(3) UNSW Law Journal 1185 at page 21 of 37 (second paragraph) under sub-heading "*Conclusion*".

always been retrievable under a search warrant. The purpose of a compelled production order is not to broaden law enforcements' powers; it is to restore them to the position they were in little more than a decade ago. In a recent article, Adam and Barns ask: 'If an individual cannot be compelled to answer questions put to them by police officers, why would it be appropriate to compel an individual to unlock their electronic device ?[7] *The question is misconceived. All jurisdictions examined in this article recognise the distinction between real, pre-existing evidence such as fingerprints, breathalyser samples and DNA tests on the one hand, and testimonial evidence that is created through compulsion, such as oral testimony, on the other hand. An encryption key is not created when it is spoken by a suspect – it already exists. So much has been recognised by the Court of Appeal of England and Wales.*[8] *It is for that reason that the Court of Appeal has upheld the lawfulness of compelled production orders. Unfortunately, the question asked by Adam and Barns appears to ignore this distinction*".

Definition of computer

80. Separately, the applicant also contends that the two smartphones are not computers and are therefore not captured by sections 48 and 49 of the 2001 Act. This raises an important issue of statutory interpretation. Specifically, the applicant has queried

[7] Lisanne Adam and Greg Barns, "Digital Strip Searches in Australia: A threat to the Privilege against Self-Incrimination" (2020) 45(3) *Alternative Law Journal* 222, 225.

[8] *R v S (F)* (n 79) 1496 [20] (Lord Judge C.J., Penry-Davey and Simon JJ.).

whether the mobile phones which were seized come within the definition of "computer" for the purposes of section 48(5) and 48(8) of the 2001 Act with the latter provision stating that "*in this section* [section 48 of the 2001 Act dealing with search warrants] *"computer at the place which is being searched'*" includes any other computer, whether at that place or at any other place, which is lawfully accessible by means of that computer.

81. It will be recalled that the applicant had been requested, pursuant to section 48(5) of the 2001 Act, to give to the member of An Garda Síochána the passwords necessary to operate the two mobile smartphone devices, being a Google Pixel 4 mobile phone and a Google Pixel 6 mobile phone, and the Asus laptop.

82. In *DPP v Crawford* [2024] IESC 44, the Supreme Court (in judgments delivered by Hogan J. and Donnelly J.) held that where an accused raises the defence of self-defence in response to a charge of murder the applicable law is set out in the provisions of s. 18 of the Non-Fatal Offences Act 1997 and the appeal of Mr. Crawford's conviction was dismissed on the basis that jury at trial had already determined that the appellant did not hold an honest belief that he had to use the level of force that he actually used. In her judgment in *DPP v Crawford*, Donnelly J. recalled that the Supreme Court had made clear in a number of authorities[9] that *language, context and purpose* were potentially in play in every exercise in statutory interpretation, none ever operating to the complete exclusion of the other:

[9]*People (DPP) v AC* [2021] IESC 74, [2022] 2 I.R. 49, *Heather Hill Management Company v An Bord Pleanála* [2022] IESC 43, [2022] 2 I.L.R.M. 313, *A, B and C v The Minister for Foreign Affairs and Trade* [2023] IESC 10, 1 I.L.R.M. 335.

> "*The starting point in the construction of a statute is the language used in the provision under consideration, but the words used in that section must still be construed having regard to the relationship of the provision in question to the statute as a whole, the location of the statute in the legal context in which it was enacted, and the connection between those words, the whole Act, that context, and the discernible objective of the statute. The court must thus ascertain the meaning of the section by reference to its language, place, function and context, the plain and ordinary meaning of the language being the predominant factor in identifying the effect of the provision but the others always being potentially relevant to elucidating, expanding, contracting or contextualising the apparent meaning of those words*".[10]

83. In *Heather Hill v An Bord Pleanála* [2022] IESC 43, the Supreme Court (Murray J.), from paragraphs 113 to 116, set out the approach to be followed which, in summary, involved applying a set of rules and presumptions the common law and legislation had developed for that purpose[11] and the application of transparent, coherent and objectively ascertainable principles to the interpretation of legislation rather than a construction based on a subjective normative judicial assessment of what the legislature wished to achieve by the legislation.

[10] *A, B and C v The Minister for Foreign Affairs and Trade* [2023] IESC 10, 1 I.L.R.M. 335 per Murray J. at paragraph 73.

[11] *DPP v Flanagan* [1979] I.R. 265 at p. 282 per Henchy J.

84. In assessing whether the two smartphones are computers and are captured by sections 48 and 49, the language and structure of the 2001 Act, as a composite statute, are important considerations. In *Heather Hill* (at paragraph 115) Murray J. emphasised that *the words of a statute* – in this case the 2001 Act – are given primacy within framework as they are the sole identifiable and legally admissible outward expression of the members of parliament's objectives:

> "*the text of the legislation is the only source of information a court can be confident all members of parliament have access to and have in their minds when a statute is passed. In deciding what legal effect is to be given to those words their plain meaning is a good point of departure, as it is to be assumed that it reflects what the legislators themselves understood when they decided to approve it*".

85. Accordingly, the Long Title to the Criminal Justice (Theft and Fraud Offences) Act 2001 refers to an "*Act to amend the law relating to the stealing and related offences and their investigation and trial; to give the force of law to provisions of the Convention on the Protection of the European Communities' Financial Interests done at Brussels on 26 July 1995 and the three Protocols to that Convention; and to provide for consequential and related matters.*"

86. Part 1, sections 1 to 3 of the 2001 Act deals with a number of preliminary matters with enactments repealed at Schedule 1. The definition of document in section 2 of the 2001 Act (Interpretation (general)) includes "*a reproduction in permanent legible form, by a computer or other means (including enlarging), of information in non-legible form.*"

87. Part 2, sections 4 to 15 of the 2001 Act deals with theft and related offences.

88. Within these provisions, section 9 of the 2001 Act creates an offence for the unlawful use of a computer: section 9(1) provides that a person who dishonestly, whether within or outside the State, operates or causes to be operated a computer within the State with the intention of making a gain for himself or herself or another, or of causing loss to another, is guilty of an offence; section 9(2) provides that a person guilty of an offence under this section is liable on conviction on indictment to a fine or imprisonment for a term not exceeding 10 years or both.

89. Part 3, sections 16 to 23 of the 2001 Act deals, *inter alia*, with the handling, possession of stolen property and other proceeds of crime.

90. Part 4, sections 24 to 31 of the 2001 Act deals with forgery.

91. Part 5, sections 32 to 39 of the 2001 Act deals with counterfeiting. In the interpretation provisions, section 32 of the 2001 Act defines "*counterfeiting instrument*" as including any instrument, article, computer programme or data, and any other means specially designed or adapted for making a counterfeit of a currency note or coin and "*currency instrument*" as including any instrument, article, computer programme or data, and any other means specially designed or adapted for making a currency note or coin.

92. Part 6, sections 40 to 47 of the 2001 Act provide for the Convention on Protection of European Communities' Financial Interests and further EU measures in this regard dealing with financial interests. Repeals of legislation are addressed at Schedules 2 to 9 of the 2001 Act.

93. Part 7 (sections 48 to 52) of the 2001 Act deals with the investigation of offences. In contrast to the position in *The People (DPP) v Quirke* [2023] IESC 5 (20th March 2023), where neither *the warrant* on foot of which the search was carried out nor *the sworn information* grounding that the warrant made any reference to digital devices, such as computers (including mobile phones), section 48(5) of the 2001 Act (which is sought to be challenged in this case) expressly anticipates a scenario where a garda acting under the authority of a warrant issued pursuant to section 48 may (a) operate any computer *at the place which is being searched* or cause any such computer to be operated by a person accompanying the member for that purpose, and (b) require any person at that place who appears to the member to have lawful access to the information in any such computer (i) to give to the member any password necessary to operate it, (ii) otherwise to enable the member to examine the information accessible by the computer in a form in which the information is visible and legible.

94. Notably, section 48(5) of the 2001 Act is only operable at the particular point in time and place which is being searched. Further, in this regard, section 48(8) of the 2001 Act provides that in "*this section, unless the context otherwise requires "computer at the place which is being searched" includes any other computer, whether at that place or at any other place, which is lawfully accessible by means of that computer.*"

95. In *The People (DPP) v Quirke* [2023] IESC 5 (20th March 2023), Charleton J. (at paragraph 82) refers to extracts of the judgment from Roberts C.J. in *Riley v California* 573 US 373 (2014) at pp. 17-19, where Roberts C.J. *inter alia* observed that "[t]*he term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone*", (and at paragraph 83) to *Dotcom, Batato, Ortmann and van der Kolk v R* [2014] NZSC 199, in emphasising "*the huge range of data that is encompassed in computer devices and how it is way outside the range of material protected even within the most extensive family, or criminal, archive.*"

96. Here, unlike the position in *The People (DPP) v Quirke*, there was no failure in the duty "*by those applying to at least mention that computerised searches for a particular purpose were central to the concerns of the proposed search party*" (*The People (DPP) v Quirke* [2023] IESC 5 per Charleton J. at paragraph 85) when the search warrant was issued by the District Court on 8th January 2024 pursuant to section 48 of the 2001 Act in relation to Apartment 7, St. Raphael's Apartments, St. Raphael's Road, Kilmacud Road Upper, Stillorgan, Co. Dublin. As set out earlier, the sworn Information referred *inter alia* to "*The application for a warrant under these provisions is an operational one as a warrant under Section 48 of this Act allows for the requirement of the provision of passwords etc. on computers (which includes mobile phones)*" and both it and the subsequent search warrant expressly referred *inter alia* to "*electronic devices including PCs, laptops, tablets, mobile phones, printers* and "*any other item(s) identified as being relevant to the investigation.*" Importantly, therefore, the sworn Information – upon which the subsequent warrant issued by the District Court on 8th January 2024 – made express reference to

requirement of the provision of passwords on computers which included mobile phones and both documents thereby signalled that garda inquiry would involve "*the digital space*" or "*virtual space*": *The People (DPP) v Quirke* [2023] IESC 5 per Charleton J. at paragraphs 28, 46, 47, 51, 52, 53 and 54.

97. In that context, and having regard to the facts as outlined, the request for passwords to unlock the smartphones and laptop arose on foot of a search warrant issued by a District Court Judge predicated on a sworn Information which were underpinned in legislative provisions which are reasonable and proportionate in the circumstances. By analogy, the sworn information and the subsequent warrant that issued in this case are consistent with the following observations of Charleton J. (at paragraph 89 of the judgment of the Supreme Court) in *The People (DPP) v Quirke* [2023] IESC 5:

> "*the intervention of a judicial mind; the need for a statutory power; the conformance with the parameters of such power; the need to specify what is in reality sought; and the duty to use a power only for the purpose for which it is granted by statute. Such an approach is necessary to ensure that the manner in which a warrant is obtained, authorising a significant but proportionate and necessary infringement on privacy rights, remains a legitimate balancing exercise carried out by the issuing judge*".[12]

[12] See also *Damache v DPP* [2012] IESC 11 per Denham C.J. at paragraph 51, [2012] 2 I.R. 266 at p. 283; *The People (DPP) v Behan* [2022] IESC 23.

98. In addition, section 52 of the 2001 Act provides for a court order directing the production of evidential material with section 52(3) specifically providing that "[w]*here the material consists of or includes information contained in a computer, the order shall have effect as an order to produce the information, or to give access to it, in a form in which it is visible and legible and in which it can be taken away.*"

99. Part 8, sections 53 to 57 of the 2001 Act deals with the trial of offences. Part 9 (sections 58 to 65) of the 2001 Act provides for a range of miscellaneous matters.

100. Having regard to the above, I consider that the ordinary and natural meaning of the words used in the 2001 Act applies to those devices, including a Google Pixel 4 mobile smartphone, a Google Pixel 6 mobile smartphone and a Asus laptop, seized during the execution of a 'section 48' search warrant informed by a 'section 48' sworn Information.

101. In addition, I consider that the following matters are relevant when considering the context and purpose of the provisions in sections 48 and 49 of the 2001 Act.

102. Section 6 of the Interpretation Act 2005, addresses how one construes legislative provisions on changing circumstances and provides:

> "*In construing a provision of any Act or statutory instrument, a court may make allowances for any changes in the law, social conditions, technology, the meaning of words used in that Act or statutory instrument and other relevant matters, which have occurred since the*

date of the passing of that Act or the making of that statutory instrument, but only in so far as its text, purpose and context permit."

103. Section 48(8) of the 2001 Act provides that unless the context otherwise requires "*computer at the place at which it is being searched includes any other computer, whether at that place or any other place, which is lawfully accessible by means of that computer.*"

104. The Merriam-Webster Dictionary online defines a computer as "*a programmable usually electronic device that can store, retrieve and process data.*" The Cambridge dictionary online defines computer as "*an electronic machine that calculates data very quickly used for storing, writing, organising and sharing information electronically or for controlling other machines.*"

105. Generally, the exercise of describing changes in the law, social conditions, technology and the meaning of words used insofar as the text, purpose and context permit, were, by analogy, encapsulated by Charleton J.'s reference in *The People (DPP) v Quirke* to *Riley v California* 573 US 373 (2014) at pp. 17-19, where Roberts C.J. *inter alia* observed that "[t]*he term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone*".

106. In addition, insofar as the specific devices the subject of this judicial review challenge are concerned, Detective Sergeant Ryan, in his Affidavit sworn on 9th July

2024, described the Google Pixel 4 mobile device and the Google Pixel 6 mobile device.

Google Pixel 4 Mobile Device

107. Detective Sergeant describes this mobile telephone as follows:

"*(17) I say that this mobile device is an electronic device, that operates using electronic circuits and components and contains a battery for powering its operation.*

(18) This device utilises an Android Operating System to control and manage the usage of the various applications and programs stores and running on the device. This device is programmable, in that it can be programmed or customised to perform particular tasks. This is frequently carried out through the installation of applications onto the device, enabling it to conduct task-specific operations.

(19) This device has a data storage capability, with various storage options of 64Gb and 128Gb available, depending on the version selected. In addition, the device has internet connectivity, allowing it to connect to Cloud based storage services.

(20) This device has a Central Processing Unit (CPU) that is used to process and conduct computations. This CPU is contained in the system on chip Qualcomm Snapdragon 855 chip set and consists of a

2.84GHz+1.78GHz 64-BIT OCTA-CORE CPU and an Adreno 640 Graphical Processing Unit (GPU).

(21) This device allows the sharing of information electronically, through the various native and third party applications including email, messaging and internet connectivity. This device can be further used to control other machines utilising network connectivity.

(22) This device contained a touch screen for the purpose of data input and allows inputted data to be written to the device, stored for later retrieval and shared utilising various applications on the device.

(23) The device's data output options, which include display to screen, printing and the sending of the data to other devices utilising various data transmission applications and protocols."

Google Pixel 6 Mobile Device:

108. Detective Sergeant Ryan then addressed Google Pixel 6 mobile device as follows:

"*(24) In respect of the Google Pixel 6 mobile device, I say that is an electronic device, that operates using electronic circuits and components and contains a battery for powering its operation.*

(25) This device utilises an Android Operating System to control and manage the usage of the various applications and programs stored

and running on the device. This device is programmable, in that it can be programmed or customised to perform particular tasks. This is frequently carried out through the installation of applications onto the device, enabling it to conduct task-specific operations.

(26) This device has a data storage capability, with various storage options of 128Gb and 256Gb available, depending on the version selected. In addition, the device has internet connectivity, allowing it to connect to Cloud based storage services.

(27) This device has a Central Processing Unit (CPU) that is used to process and conduct computations. This CPU is contained in this system-on-chip Google Tensor chip set and consists of a 64-BIT OCTA OCTA-Core (2x2.80 GHz Cortex-X1&2x2.25GHz Cortex-A76&4x1.80GHz Cortex-A55) CPU and a Mali-G78 MP20 Graphical Processing Unit (GPU).

(28) This device allows the sharing of information electronically through the various native and third party applications including email, messaging and internet connectivity. This device can be further used to control other machines utilising network connectivity.

(29) This device contains a touch screen for the purpose of data input and allows inputted data to be written to the device, stored for later retrieval, and shared utilising various applications on the device.

(30) The device has data output options, which include display to screen, printing and the sending of the data to other devices utilising various data transmission applications and protocols.

(31) With reference to outlining the way in which either of the above mobile devices actually carry out their particular functions, and the manner in which these devices actually operate in specific technical detail, this is beyond my area of expertise, which is confined to the forensic examination of digital devices and the extraction analysis of the content from such devices on an evidential attribution basis".

109. In addition, therefore, I consider, having regard to the context and purpose of the provisions in sections 48 and 49 of the 2001 Act, that these provisions apply to a Google Pixel 4 mobile smartphone, a Google Pixel 6 mobile smartphone and an Asus laptop, which devices were seized during the execution of the warrant in this case.

CONCLUSION

110. The applicant's Statement of Grounds had also sought a declaration pursuant to section 5 of the ECHR Act 2003 to the effect that sections 48(5)(b)(i), 49(1)(c) and 49(2) of the 2001 Act were incompatible with the State's obligations under Articles 6 and 8 of the ECHR.

111. Under the sub-heading '[i]*ncompatability of the impugned sections with the Respondent's obligations under the ECHR Act 2003*', the following is set out at paragraphs 26, 27 and 28 of the Statement of Grounds: "*(26)* [t]*he said sections are also incompatible with the State* [r]*espondents' obligations to enact laws compliant with Articles 5, 6 and 8 ECHR, as provided for in Irish law under section 5 of the ECHR Act 2003'; (27) '*[t]*he caselaw of the* [ECtHR] *in cases such as Funke v France (App no 10928/84 (ECHR 25 February 1003), and JB v Switzerland, App no 31827/96 (ECHR 3 May 2001) make clear that privilege against self-incrimination is an essential aspect of Article 6 ECHR. The privilege extends beyond testamentary utterances, to protect suspects who are coerced into identifying and/or handing over documentary material that would tend to incriminate them'; (28) [the privilege applies a fortiori where the coercive power involves the threat of prosecution and imprisonment]*".

112. In addition, to a stay and interim/interlocutory relief, the Statement of Grounds sought damages for the alleged breach of the applicant's constitutional rights and for false imprisonment and, in the alternative, damages pursuant to section 3 of the ECHR Act, 2003,[13] having regard to the alleged failure of the State respondents to comply with the requirements of Articles 5, 6 and 8 ECHR.

[13] The Statement of Grounds under the sub-heading "*Damages*" *inter alia* states at paragraph (39) that "[t]*he process of coercion he endured, and the criminal process he has been subject to, have adversely impacted on the* [a]*pplicant's psychological well-being and on his good name; in a manner which requires full vindication pursuant to Article 40.3.2 of the Constitution or in the alternative, pursuant to section 3 of the ECHR Act 2003*."

113. Notwithstanding the references in the Statement of Grounds to section 5 of the ECHR Act 2003 and the alternative ground in relation to damages pursuant to section 3 of the ECHR Act 2003, as indicated at the beginning of this judgment, the submissions made on behalf of the applicant at the hearing of this judicial review application focused on seeking declaratory relief that section 48(5)(b)(i), section 49(1)(c) and section 49(2) of the 2001 Act were unconstitutional, contending that these statutory provisions amounted to a disproportionate interference with the applicant's asserted right to the privilege against self-incrimination.

114. In terms of the central challenge in fact made in these proceedings, that focus reflects the observations of the Supreme Court in a series of judgments – *Corcoran & Anor v The Garda Commissioner & Anor* [2023] IESC 15, *Gorry v Minister for Justice* [2020] IESC 55, *Clare County Council v McDonagh* [2022] IESC 1, [2022] 2 I.R. 122, *Middlekamp v Minister for Justice* [2023] IESC 3, [2023] 1 I.L.R.M. 277, *Odum v Minister for Justice* [2023] ISEC 26 – which emphasise that, *as a matter of substance*, the seeking of a declaration of unconstitutionality is not the same as the seeking of a remedy under section 5 of the ECHR Act 2003 as the former, if granted by a court, has immediate, *erga omnes* prospective effect, famously described by Henchy J. as the equivalent of a "*judicial death certificate*" in *Murphy v Attorney General* [1982] IR 241 at p. 340, whereas section 5(2) of the ECHR Act 2003 *inter alia* provides that the granting of a *declaration of incompatibility* shall not affect the validity, continuing operation or enforcement of the statutory provision or rule of law in respect of which it is made, *and as a matter of procedure or priority*, the first port of call should always be the constitutional challenge.

115. The issue in this application for judicial review raised what was in essence an '*obstruction prosecution*' in the context of where members of An Garda Síochána – acting under the authority of a lawful search warrant to operate any computer found at the place which was being searched – required the applicant – who was present at that place and who owned the computers which were seized and which comprised a Google Pixel 4 mobile smartphone, a Google Pixel 6 mobile smartphone and an Asus laptop – to furnish any passwords necessary to operate them and he refused.

116. In terms of the applicant's argument that the process lacked sufficient judicial supervision, the search warrant in this case was issued on foot of a detailed sworn Information pursuant to the provisions of section 48 of the 2001 Act and which had informed the District Judge, who issued the warrant, that it may include *inter alia* digital devices, such as computers (including mobile phones). As mentioned earlier, the sworn Information – upon which the subsequent warrant issued by the District Court on 8th January 2024 – made express reference to requirement of the provision of passwords on computers which included mobile phones and both documents thereby signalled that garda inquiry would involve "*the digital space*" or "*virtual space.*"

117. Further, (as just stated) it was not in dispute that the applicant was in fact *the owner* of the devices in question the subject of the search on foot of the lawful search warrant which was issued by the District Court, *i.e.*, the Google Pixel 4 mobile smartphone, a Google Pixel 6 mobile smartphone and a Asus laptop, and therefore, had "*lawful access to the information in any such computer.*"

118. The power to request the applicant to give the member of An Garda Síochána any passwords necessary to operate the devices was under the authority of the search warrant issued pursuant section 48 of the 2001 Act which was predicated on a sworn Information and is expressly provided for in section 48(5)(b)(i) of the 2001 Act. Further, and in relation to the argument made on behalf of the applicant that the password did not have to be given *'there and then'*, the power to request the applicant to give the member of An Garda Síochána any password necessary to operate the phone or computer occurs *at the time* and *at the place which is being searched* (as per the reference in section 48(5) of the 2001 Act).

119. For the reasons which are set out in this judgment, I have found that the privilege against self-incrimination was not engaged in this case. The Google Pixel 4 mobile smartphone, the Google Pixel 6 mobile smartphone and the Asus laptop were all computers as envisaged in section 48 of the 2001 Act and the passwords in relation to each of these three devices existed independent of the will of the applicant.

120. I have also found that the Google Pixel 4 mobile smartphone, the Google Pixel 6 mobile smartphone and the Asus laptop, seized during the execution of the warrant in this case, come within the express parameters of the sworn Information and search warrant issued in this case and comprise 'computers' as referred to in section 48 and 49 of the 2001 Act.

121. Further, for the reasons set out, I do not consider that the powers in section 48(5)(b)(i) of the 2001 Act (which confers the power to require the applicant to provide passwords for the three devices), section 49(1)(c) of the 2001 Act (which

creates an offence when failing to comply with this requirement), and section 49(2) of the 2001 Act (which provides for the power of arrest) are invalid, having regard to the Constitution, or that they amount to a disproportionate interference with the applicant's asserted right to the privilege against self-incrimination.

122. The applicant fully accepts that he is *the owner* of the Google Pixel 4 mobile smartphone, the Google Pixel 6 mobile smartphone and the Asus laptop which are now in the *lawful* possession of the gardaí have been seized on foot of a lawful warrant which (a) has *not* been challenged in these proceedings and (b) where the underpinning legislative basis on which the warrant issued has also *not* been challenged.

123. The question of damages, therefore, does not arise, and insofar as a declaration is sought pursuant to section 5 of the ECHR Act 2003 as per the applicant's Statement of Grounds, for the reasons set out above, I refuse a declaration under those provisions.

124. In the circumstances, therefore, I refuse the applicant's application for the reliefs sought by way of judicial review.

PROPOSED ORDER

125. I shall make an order refusing the applicant's application for the reliefs claimed by way of judicial review.

126. I shall put the matter in before me at 10:15 on Friday 20th December 2024 to deal with final orders, including the question of costs.

CONLETH BRADLEY

11th December 2024