

**THE SUPREME COURT**

Appeal No 5/2022

BETWEEN

**THE DIRECTOR OF PUBLIC PROSECUTIONS**

**RESPONDENT**

**AND**

**PATRICK QUIRKE**

**APPELLANT**

**AND**

**THE IRISH HUMAN RIGHTS AND EQUALITY COMMISSION**

**AMICUS CURIAE**

**SUBMISSIONS ON BEHALF OF THE AMICUS**

**Introduction**

1. In this submission, the *amicus curiae* (the ‘Commission’) addresses whether specific safeguards are required in respect of the seizure of electronic devices pursuant to a search warrant, and whether such safeguards can be read-in to the search warrant power used in this case.
2. S.10 of the Criminal Justice (Miscellaneous Provisions) Act 1997 as amended, is the most commonly used search warrant power. The section requires consideration of whether ‘*there are reasonable grounds for suspecting that evidence of, or relating to, the commission of an arrestable offence is to be found*’. If so found, a District Judge ‘*may*’ proceed to issue a search warrant.
3. S.10 is silent, however, in respect of any proportionality considerations to which the Judge should have regard. How, therefore, is privacy in respect of electronic devices to be accommodated, alongside the community’s interest in the detection and prosecution of crime?
4. In other common law countries, the search warrant application involves a detailed review of what is suspected will be found during a search and why it is intended to be seized. The basis for an application must be fully set out and recorded, with a considerable duty of candour on the part of the person seeking the warrant. Sometimes, limitations are imposed on the extent to which electronic devices can be accessed. In contrast, Irish search warrant provisions are relatively blunt instruments.
5. It is submitted, nonetheless, that the statutory power in this case can be interpreted so as to read-in certain safeguards: in particular, a duty of candour and a requirement to specify all relevant matters that touch upon the proportionality of issuing a search warrant.

6. The fact that a computer or other electronic device may be seized is one such relevant matter. Given the scope of the interference with privacy occasioned when a computer is seized, it is vital that the warrant-issuer be informed of why seizure is deemed necessary.
7. The Commission seeks to highlight caselaw and practice from the United States, the United Kingdom and the European Court of Human Rights ('ECtHR'), not already referred to by the parties. This material demonstrates that there may be a deficit in the way privacy rights are protected in the search warrant process in this jurisdiction, in respect of electronic devices.

#### **Irish case-law in respect of the protection of privacy in the context of search warrants**

8. In the recent case of *Akram v Minister for Justice*<sup>1</sup>, Ni Raifeartaigh J highlighted the growing complexity associated with the seizure of electronic devices. She pointed out that the seizure process will involve various stages:

*'... while lawyers sometimes speak of 'search and seizure' generically, the reality is that the overarching concept of 'search and seizure' encompasses a large number of distinct component actions or tasks by the searching party. This is particularly so in the modern context of digital information storage as a result of technological advances in the last number of decades. Information may now be stored on, and accessed from, a wide range of digital devices. The original paradigm of physically taking possession of a document and reading it no longer applies where digital information is in issue. The reality is that the broad concept of 'search and seizure' might involve some or all of the following individual steps (and no doubt this list is itself incomplete):*

*(i) Entry onto premises (whether a dwelling or other premises);*

*(ii) Search of a person;*

*(iii) Search of an object connected with a person, such as an item of luggage or clothing;*

*(iv) Reading paper document(s);*

*(v) Reading information on a smartphone or laptop which is not password protected, such as messages or emails;*

*(vi) Taking possession of devices such as smartphones or laptops which are password protected;*

*(vii) Taking possession of other forms of digital storage such as hard drives, CD-ROMs, USB sticks and the like;*

<sup>1</sup> [2022] IECA 108, at paragraph 5 of her partially-dissenting judgment.

(viii) *Taking copies of the entirety of the digital information on a device (such as copying a hard drive);*

*Taking copies of individual pieces of information on a device (such as taking a screenshot of individual messages on a phone);*

(x) *Sorting potentially relevant material from potentially irrelevant material (by “relevant”, I mean relevant to the task in hand or the purpose for which the search and seizure was carried out, e.g. a fraud investigation, a drugs investigation, an immigration decision, and so on);*

(xi) *Sorting potentially legally privileged material from non-privileged material;*

(xii) *Retaining information/copies of information thereby obtained or devices;*

(xiii) *Destroying information;*

(xiv) *Returning information or devices.’*

9. Other jurisdictions have regimes that address these various stages of the seizure process, ensuring a holistic approach to privacy protection. Even if a search is permitted, interference with privacy rights may still be mitigated during the process.

10. In the case of *CRH v Competition Commission*<sup>2</sup>, Charlton J referred to the difficulties in accommodating both privacy rights and community interests in the context of a search:

*‘It is inevitable that in granting a warrant, intrusions into the private space occur. It is certain that matters outside those of even potential relevance to a criminal or regulatory investigation will come to the attention of those authorised to search. Even entering an office, there may be family mementos or other personal items, while a legally-mandated entry into a dwelling is far wider than the access normally granted to any visitor and is revelatory of life choices. Visitors are generally confined to one room, a kitchen or a living room, while those who search must necessarily look at bedrooms and inside cupboards or under floorboards. Hence, the importance of the interposition of judicial scrutiny to authorise such intrusions. That judicial authorisation is only given where the statutory parameters are fulfilled to satisfy the necessity for the search; most usually that of reasonable suspicion about a crime that has been perpetrated or is in planning. Mirroring the nature of entry into the private space which a judicially authorised search engages, the taking or copying of records, of data or email necessarily moves into the private space. But, it may be necessary and that depends on the nature of what suspicion is held and the nature of the crime. It may be proportionate because of the nature of investigations, conducted as they are for the benefit of society for the detection of crime, with a view to gathering both what will assist a prosecution and what may offer a defence to an accused. An investigation, for example, into child pornography offences will almost invariably require the seizing of a suspect's computer. That is necessary. As in all criminal investigations, other rights are engaged, most obviously that of the protection of the life and bodily and mental integrity of victims. In addition, there is the duty of all democratic states to have a*

<sup>2</sup> [2018] 1 I.R. at p.644.

*functioning criminal justice system, founded on reason and on clear rules to which the victims of crime can have recourse. Embedded in that computer will perhaps be material outside the scope of constitutionally-mandated privacy, the images that constitute the nature of the charge; that is what the investigators are seeking to establish. Also included will be legitimate and private communications with friends, photographs of social occasions and perhaps documents or literary efforts of the suspects. In due course, only what is relevant and what has the ability to provide assistance to the prosecution or the defence will be focused on, the remaining material will be winnowed out as unimportant. That why the computer was seized in the first place. Its seizure was proportionate and the necessity to examine what is on it is justified by the nature of the investigation. Similarly, with the investigation of a terrorist offence, the nature of what has been done, or what needs to be uncovered where a planned outrage is suspected, may similarly justify such complete scrutiny as requires the copying of an email account or the downloading of the hard drives of multiple computers.'*

11. While acknowledging the significant community interest in the detection of crime, and that this inevitably entails incursions into the private space, Article 40.5 of the Constitution is in particularly strong terms. The dwelling is *'inviolable... save in accordance with law'*. A process that leads to such incursion therefore requires close scrutiny, in terms of both legislation and practice.
12. A similar approach is taken in the ECHR jurisprudence. In both the constitutional and Convention analysis, proportionality is a key consideration. The availability of safeguards is an indicator of whether a search power is proportionate.
13. The strength of the Article 40.5 protection of the dwelling was emphasised by Hogan J in *Schrems v Data Protection Commissioner*<sup>3</sup>. While the context is different here - involving a targeted interference with electronic data, rather than the potential mass surveillance at issue in *Schrems* - Hogan J's comments show the strength of the protection afforded to privacy enjoyed within the dwelling:

*'[50]... interference with these privacy interests must be in a manner provided for by law and any such interference must also be proportionate. This is especially the case in respect of the interception and surveillance of communications within the home. While the use of the term "inviolable" in respect of the dwelling in Article 40.5 does not literally mean what it says, the reference to inviolability in this context nonetheless conveys that the home enjoys the highest level of protection which might reasonably be afforded in a democratic society: see, e.g., Wicklow County Council v. Fortune.'*

*[53]... As Hardiman J. observed in The People (Director of Public Prosecutions) v. O'Brien [2012] IECCA 68, (Unreported, Court of Criminal Appeal, 2nd July, 2012), Article 40.5:-*

*"17 ... presupposes that in a free society the dwelling is set apart as a place of repose from the cares of the world. In so doing, Article 40.5 complements and reinforces other constitutional guarantees and values,*

<sup>3</sup> [2014] 3 IR 75 at p.94.

*such as assuring the dignity of the individual (as per the Preamble to the Constitution), the protection of the person (Article 40.3.2°), the protection of family life (Article 41) and the education and protection of children (Article 42). Article 40.5 thereby assures the citizen that his or her privacy, person and security will be protected against all comers, save in the exceptional circumstances presupposed by the saver to this guarantee.”*

*[54]One might accordingly ask how the dwelling could in truth be a “place of repose from the cares of the world” if, for example, the occupants of the dwelling could not send an email or write a letter or even conduct a telephone conversation if they could not be assured that they would not be subjected to the prospect of general or casual state surveillance of such communications on a mass and undifferentiated basis.’*

14. Where, for example, a family uses a communal computer within the home, the private content thereof must remain inviolable: except where the proportionality of the interference has been clearly demonstrated, following a process wherein their privacy rights have been properly considered.
15. It is submitted that there is scope to accommodate greater protection of privacy than is apparent on the plain words of the most commonly-used statutory search powers. In particular, precision as to what is to be seized, and why it is to be seized, ought to be treated as a basic requirement in a warrant application.
16. In other jurisdictions, the requirement to identify with precision the subject-matter of the search is a basic requirement. Clearly, it is not possible in every case to predict what will be found. But there could not be a reasonable suspicion that evidence will be found unless there are indicators, in support of that suspicion, that at least some specific items may be found.
17. While there has been limited analysis of this issue in Irish caselaw, there is some acknowledgment that the items being sought should be specified in the warrant request in so far as possible. The Court of Appeal, in the instant case, were alive to this concern. They commented that it had been ‘*sub-optimal*’ that the computer had not been referenced on the sworn information.
18. Charleton J in *CRH* approved of *dicta* from CJEU caselaw, that there is an obligation to specify with precision in a warrant application both the ‘*subject-matter*’ and the ‘*purpose*’ of the search:

*[258] Central to the protections afforded to an undertaking or individual searched pursuant to warrant is that there should be judicial authorisation for such an intrusion and that the information grounding the search be sufficiently precise as to the target of the inquiry; Nexans v. Commission (Case T-135/09)[2013] 4 C.M.L.R. 195. As the General Court observed at p. 212:-*

*“39 The obligation on the Commission to specify the subject-matter and purpose of the inspection is a fundamental requirement in order both to show that the investigation to be carried out at the premises of the undertakings concerned is*

*justified, enabling those undertakings to assess the scope of their duty to co-operate, and to safeguard the rights of the defence.”*

*[259] This protection was present in this case, as it is in all criminal law searches in this jurisdiction.’*

19. In *DPP v Balfe*<sup>4</sup>, the Court of Criminal Appeal observed:

*‘Neither counsel on behalf of the applicant nor counsel on behalf of the Director of Public Prosecutions could find any authority as to the effect of omitting to identify the goods the subject matter of a search warrant...*

*It is, however, the opinion of this Court, notwithstanding the paucity of authority, that the very concept of an application for and the granting of a warrant to search for stolen goods involves the provision of some description of the goods stolen and the goods for which it is intended to search.’*

20. The caselaw appears to show that if some plausible basis has been put forward for a search in the short written information provided, a warrant will usually be granted without further detailed analysis or interrogation. The lack of rigorous examination of the grounds for a search may be a reflection of the lack of express safeguards in the process. Nonetheless, a warrant-issuer can probe the limited written information provided in support of the warrant application.
21. In this jurisdiction, the most common search warrant provisions do not contain express stipulation that an issuing authority may request further information from the applicant. In contrast, in England and Wales, the Police and Criminal Evidence Act 1984 (‘PACE’) provides that an applicant *‘shall answer on oath any question that the justice of the peace or judge hearing the application asks him.’* Similar provisions can be found in Australian law<sup>5</sup>.
22. While there is no such express power, District Judges and Peace Commissioners do sometimes interrogate the reliability of the sworn information. This practice has been acknowledged in the caselaw: see *DPP v Kenny*<sup>6</sup>.
23. However, any additional questions put and any answers given are rarely, if ever, recorded and available for consideration in a criminal trial. This does little to enhance the prospects of procedural fairness.
24. It is submitted that there is a duty of candour on the part of the warrant-seeker to set out any relevant matters that may count against the issuing of the warrant: for example, if the persons residing at the dwelling are not themselves suspects; or are a family, with children likely to be present; or if the suspect is of previous good character; or if the informant providing the intelligence has not provided information previously; or if the dwelling has been searched previously, without success.

<sup>4</sup> [1998] 4 I.R. 50 at p.61.

<sup>5</sup> In statutory provisions applying in New South Wales, Victoria, and Queensland.

<sup>6</sup> [1990] 2 IR 110, per Lynch J at p.141.

25. The same duty of candour should apply, it is submitted, when electronic devices are to be seized.
26. This does not appear to be the current practice, at least in the context of the sworn written information provided. It is therefore important, in order to ensure compliance with the duty of candour, that there would be an accessible record kept of what has been said.
27. The Court of Appeal decision in *Corcoran* was in the different context of journalistic privilege. But it highlights the necessity for sufficient information to be provided to the warrant-issuer, so that they can properly assess the interests and rights at issue. Costello J said<sup>7</sup>:

*'It is essential that a District Court judge is able to balance fairly the interests of the public in the investigation of serious crime, in this instance, and the rights of the journalist and his or her sources, on the other hand and then decide which of two competing interests is to prevail. If the court is not alerted to the fact there is such a clash of interests, it cannot resolve it. Likewise, if it does not have a complete picture of the facts as then known to the applicant for the warrant, the court is most unlikely to be able to balance these competing rights in accordance with the requirements of the Constitution and the Convention.'*

#### **EHCR principles in respect of search warrant powers**

28. Search warrant powers interfere with the privacy rights protected under Article 8 ECHR, and so a proportionality assessment is required. When determining whether the interference is 'necessary in a democratic society', the ECtHR has regard to the margin of appreciation left to the Contracting States. However, the exceptions provided for in Article 8(2) are to be interpreted narrowly, and the need for them in a given case must be convincingly established.
29. The ECtHR considers<sup>8</sup> whether the reasons adduced to justify the search are 'relevant' and 'sufficient'. This involves examining the terms in which the search warrant has been drafted and the reasons provided by domestic authorities to justify recourse to the search. The Court also considers whether the search is proportionate. This involves an examination of whether legislation and practice afford individuals adequate safeguards against abuse, in addition to whether the particular measures taken in each case are proportionate to the aim of preventing the crime alleged.
30. As noted by the Appellant, there does not appear to be a ECtHR case addressing the specific issue of whether enhanced safeguards are required in respect of seizure of electronic devices. However, *obiter* comments in the case of *Sher v United Kingdom*<sup>9</sup> suggest that this may be so.

<sup>7</sup> [2022] IECA 98 at para 136.

<sup>8</sup> *KS and MS v Germany* (2016) App no 33696/11 at [44]. See also *Buck v Germany* (2006) 42 EHRR 21 (App no 41604/98) at [45].

<sup>9</sup> Application no. 5201/11.

31. The ECtHR in *Sher* acknowledged that complexities arise in respect of the seizure of electronic devices. More generally, the Court noted that while it is desirable to identify exactly what is to be sought in a search, whether that will amount to a requirement is dependent on the context:

*'170. The third-party intervener, Privacy International, focused its comments on searches of electronic devices, which entailed access to personal and communications data. It emphasised the innovations in technology which had resulted in previously unimagined forms of collecting, storing, sharing and analysing data. Access by law-enforcement officers to an individual's electronic devices could enable access to everything that person had ever digitally touched, encompassing data not stored on the device itself but on external networked servers. The combination of data available could be extremely revelatory. In light of the particularly intrusive nature of searches of electronic devices, Privacy International argued for a high threshold when determining whether an interference with Article 8 rights was justified.'*

## *2. The Court's assessment*

*174. ... the specificity of the list of items susceptible to seizure in a search conducted by law-enforcement officers will vary from case to case depending on the nature of the allegations in question.*

*Cases such as the present one, which involve allegations of a planned large-scale terrorist attack, pose particular challenges, since, while there may be sufficient evidence to give rise to a reasonable suspicion that an attack is under preparation, an absence of specific information about the intended nature of the attack or its targets make precise identification of items sought during a search impossible. Further, the complexity of such cases may justify a search based on terms that are wider than would otherwise be permissible. Multiple suspects and use of coded language, as in the present case, compound the difficulty faced by the police in seeking to identify in advance of the search the specific nature of the items and documents sought.*

*Finally, the urgency of the situation cannot be ignored. To impose under Article 8 the requirement that a search warrant identify in detail the precise nature of the items sought and to be seized could seriously jeopardise the effectiveness of an investigation where numerous lives might be at stake. In cases of this nature, the police must be permitted some flexibility to assess, on the basis of what is encountered during the search, which items might be linked to terrorist activities and to seize them for further examination. While searches of electronic devices raise particularly sensitive issues, and arguably require specific safeguards to protect against excessive interference with personal data, such searches were not the subject of the applicants' complaints or the domestic proceedings in this case and, in consequence, no evidence has been led by the parties as to the presence or otherwise of such safeguards in English law.'*

*(underlining added)*

**U.S. caselaw requires stringent safeguards in respect of searches involving electronic devices**



32. It is worth considering the caselaw on search warrants from the United States, as it deals expressly with a number of issues relevant to this appeal that are under-developed in our own caselaw.
33. The Fourth Amendment to the United States Constitution protects people from unreasonable searches and seizures by the government. There are historical reasons, going back to pre-revolutionary times, why there has been a particular abhorrence of overbroad search powers and ‘general searches’.
34. The U.S. Supreme Court has recognised the importance of ensuring that the balance between the power of the State and the privacy of the individual is not upset due to unanticipated technological advances: *United States v Jones*.<sup>10</sup> The Fourth Amendment analysis asks whether the police conduct threatens to disrupt the traditional ‘*relationship between citizen and government in a way that is inimical to democratic society*’.
35. In this regard, the comments of Roberts C.J. in *Riley*, as cited in the Appellant’s submissions at para 62. are apt. There is a vast difference between a traditional and a digital search.
36. To obtain a search warrant, law enforcement in the U.S. must demonstrate probable cause, defined as a ‘*fair probability that contraband or evidence of a crime will be found in a particular place.*’<sup>11</sup> This approximates with our own requirement of reasonable suspicion.
37. In addition to probable cause, warrants must not be overbroad. A warrant is overbroad when it purports to authorise searches or seizures of places or things for which probable cause has not been demonstrated. An affidavit supporting a search warrant must therefore demonstrate the ‘*nexus . . . between the item to be seized and criminal behavior.*’<sup>12</sup>
38. Additionally, warrants must particularly describe the things to be searched and seized. U.S. Courts have applied the particularity requirement stringently in the context of digital data<sup>13</sup>:  
  

*‘The modern development of the personal computer and its ability to store and intermingle a huge array of one’s personal papers in a single place increases law enforcement’s ability to conduct a wide-ranging search into a person’s private affairs, and accordingly makes the particularity requirement that much more important.’*
39. The U.S. Courts have acknowledged, in the general context of searches, that the fact that evidence of a crime is often found in a particular location does not supply probable cause to believe that it will be found in that location in any particular case. Police may be refused permission to search a home without an investigation-specific reason to believe evidence will be found there. The connection must be specific and concrete, not ‘*vague*’ or ‘*generalized.*’<sup>14</sup>
40. In the same way, probable cause to issue a warrant to seize electronic devices must be based on case-specific facts. This is demonstrated by multiple decisions in U.S. state courts. For

<sup>10</sup> 565 U.S. at 416 (Sotomayor, J., concurring).

<sup>11</sup> *Illinois v. Gates*, 462 U.S. 213, 238 (1983).

<sup>12</sup> *Warden, Md. Penitentiary v. Hayden*, 387 US 294, 307 (1967).

<sup>13</sup> *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009).

<sup>14</sup> *United States v. Brown*, 828 F.3d 375 (6th Cir. 2016).

example, in *United States v. Lyles*<sup>15</sup>, the affidavit for the warrant asserted that the home, where a phone was later recovered, was connected to drug trafficking. That assertion was held to be insufficient to establish probable cause to search the phone, because it did not demonstrate the nexus between the phone and the alleged crime. In *Commonwealth v. Broom*,<sup>16</sup> a warrant to search a defendant's phone as part of a murder investigation was held to be overbroad. The affidavit did not satisfy probable cause to search the phone because the statement that the phone '*will likely contain information pertinent to this investigation*' was held to be '*general*' and '*conclusory*.'

41. In short, a proper factual nexus is required before electronic devices should be searched. It must be based on more than the fact that computers and phones can potentially be used in furtherance of crime.
42. While this caselaw might differ from our own approach, it does highlight that where electronic devices are concerned, a reasonable suspicion relied on by the warrant-seeker requires to be interrogated properly, to ask whether the justification for seizure has been properly made out.

**U.K. caselaw and statutory powers also demonstrate a greater level of safeguards**

43. U.K. law provides for more safeguards, in the context of issuing search warrants, than is expressly provided for in Irish law. Moreover, a significant duty of candour has been held to attach to *ex parte* warrant applications. The duty was described by the U.K. Supreme Court in *R (Haralambous)*<sup>17</sup> as meaning that the information on which the warrant-seeker relies must constitute a fair and balanced presentation of the circumstances.
44. In *Re Stanford International Limited*<sup>18</sup>, Hughes L.J. observed that:

*'In effect a prosecutor seeking an ex parte order must put on his defence hat and ask himself what, if he was representing the defendant or a third party with the relevant interest, he would be saying to the judge, and, having answered that question, that is precisely what he must tell.'*
45. Search warrant application forms include a box prompting applicants to provide any information that might reasonably be considered capable of undermining any of the grounds of the application. This is followed by a declaration that this has been done and a note for guidance. The guidance note gives the example of whether the premises have been searched before or whether there are unusual features of the investigation.
46. Under S.15(6)(b) of PACE, the warrant must also identify, so far as is practicable, the articles or persons sought. The House of Lords said, in *McGrath (AP) v. Chief Constable of the RUC*<sup>19</sup>, that the rationale behind section 15(6) is that '*warrants must be sufficiently clear and precise in their terms so that all those interested in their execution may know precisely what are the limits of the power which has been granted.*'

<sup>15</sup> 910 F.3d 787, 794–95 (4th Cir. 2018).

<sup>16</sup> 52 N.3d 81, 89 (Mass. 2016) Id. at 89.

<sup>17</sup> [2018] UKSC 1 *Per* Lord Mance, at para 34.

<sup>18</sup> [2010] 3 WLR 941.

<sup>19</sup> [2001] UKHL 39.

47. Further express statutory protection in respect of electronic devices has been recommended by the Law Commission in a 2020 report. They have recommended that<sup>20</sup>:

*'search warrant application forms be amended to require an investigator, who seeks to obtain a warrant to search for and seize electronic devices to acquire electronic data, to explain: (1) in as much detail as practicable what information on the devices is sought; and (2) why they believe that the information is on the devices and why the information would satisfy the statutory conditions.'*

### **Applying these principles to the search warrant power contained in S.10 of the 1997 Act as amended**

48. In *Corcoran*, Costello J acknowledged that it would be preferable if the Oireachtas had provided for an express procedure to protect journalistic privilege in the context of a search warrant applications under S.10 of the Criminal Justice (Miscellaneous Provisions) Act 1997, as amended.
49. In this regard, significant reforms have recently been proposed by the Government in respect of search warrants in the Garda Síochána (Powers) Bill 2021. These reforms reflect the recommendations of a detailed 2015 Law Reform Commission report<sup>21</sup> on search warrants.
50. There was no treatment of the specific issues raised by this case in the 2015 report. Some limited recommendations for reform were made in respect of the power contained in S.10 of the 1997 Act. It was also proposed that there should be a more generally-available search warrant power.
51. A more general search warrant power has now been proposed in the 2021 Bill<sup>22</sup>. This power substantially replicates the wording of S.10 of the 1997 Act, as amended, with some additional features. For example, the *'applicant shall provide any additional information which the judge of the District Court requests so as to ground the application'*.
52. Notably, the Bill also proposes a power to compel persons present during a search to facilitate the examination of electronic devices and to provide passwords and encryption keys.
53. The Bill seeks to address some of the concerns raised in the *CRH* case, in respect of the over-seizure of irrelevant and sensitive material. It makes provision for the retention of material that is not practicable to sort through *in situ*, but it does not prescribe any procedure for sorting sensitive material and for returning irrelevant material.

<sup>20</sup> Law Commission summary of Final report on Search Warrants, p.12  
<https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2020/10/Search-warrants-summary.pdf>

<sup>21</sup>

[https://www.lawreform.ie/\\_fileupload/Reports/Report%20on%20Search%20Warrants%20and%20Bench%20Warrants%201%20December%202015%20-%20Final%20Version.pdf](https://www.lawreform.ie/_fileupload/Reports/Report%20on%20Search%20Warrants%20and%20Bench%20Warrants%201%20December%202015%20-%20Final%20Version.pdf)

<sup>22</sup> See Heads 15 to 22 of the Bill:

[https://www.justice.ie/en/JELR/Gen\\_Scheme\\_of\\_AGS\\_\(Powers\)\\_Bill.pdf/Files/Gen\\_Scheme\\_of\\_AGS\\_\(Power s\)\\_Bill.pdf](https://www.justice.ie/en/JELR/Gen_Scheme_of_AGS_(Powers)_Bill.pdf/Files/Gen_Scheme_of_AGS_(Power s)_Bill.pdf)

54. A statutory Code of Practice is proposed to be adopted, which would assist warrant-seekers and which would ‘set-out’:

*‘(a) the scope and extent of a search of a place, (b) the scope and extent of a search of persons present at the place, (c) the particular safeguards to apply when the subject of a search is a child or a vulnerable person, (d) procedures for dealing with material that has been seized where representations have been made that the material is private and not relevant to the offence for which the investigation has been carried out, and (e) such other matters related to the search as the Commissioner deems appropriate.*

*(3) When preparing a Code of Practice under this Head, the Commissioner shall have regard to the following— (a) the obligation on members of the Garda Síochána to act with diligence and determination in the investigation of crime and the protection and vindication of the rights of victims and the protection of the public; (b) the fact that a search of a place may involve an interference in a person’s right to privacy; (c) the fact that a search of any dwelling is an interference in the inviolability of the dwelling; (d) any such search must be necessary and proportionate to the legitimate objectives to be achieved.’*

55. Returning to S.10 of the 1997 Act however, it provides no such guidance as to how issues in respect of the privacy of electronic devices should be resolved in the warrant application process or during the search. It is submitted that this is a flaw in the legislation. As Charleton J noted in *CRH*<sup>23</sup>:

*‘When addressing the conferring of powers of search or arrest, it is desirable that “broad, plain, intelligible principles” should be stated. Those tasked with the temporary deprivation of liberty that arrest involves or the intrusion into home or business which a warrant authorises, as well as those who are the subject of same, need plain guidance and clear boundaries; see the remarks of Best J. in The King v. Weir(1823) 107 E.R. 108 at p. 111.’*

56. The judgment in *Corcoran* acknowledges, however, that there is scope for providing additional information in the context of the warrant procedure under S.10, so as to ensure that constitutional rights are protected. Costello J said<sup>24</sup>:

*‘For the reasons I have set out, in my judgment s.10 may provide in some circumstances an appropriate procedure for an application for a search warrant of journalistic material or a journalist’s home or work place provided that sufficient information, both as to fact and as to law, is placed before the District Court judge to whom the application for the warrant is made. This is permissible under s.10 and therefore I do not believe that s.10 is incompatible with the Constitution and therefore the failure to seek an order that it is incompatible with the constitution is not fatal to the applicants’ case.’*

57. It is submitted that S.10 must be interpreted as requiring a similar procedure, providing ‘sufficient information’ to the Judge in respect of the intention to seize electronic devices.

<sup>23</sup> At para 233.

<sup>24</sup> At para 146.

58. Having regard to the duty of the State under Article 40.3.1 of the Constitution to respect, in its laws, the personal rights of affected persons, it is to be presumed that it was the intention of the Oireachtas that a Judge's discretion under the section would be sufficiently broad to protect such rights.
59. The Commission therefore submits that the application of the double construction rule of interpretation requires that the search warrant power at issue, S.10 of the Criminal Justice (Miscellaneous Provisions) Act 1997 as amended, be construed as requiring the warrant-seeker to refer to the fact that they seek electronic devices, and to explain why this is justified.
60. It is submitted that an alternative interpretation of the section, which does not require such disclosure, would at a minimum lead to doubts over the constitutionality of the section.
61. There are limits to how the section can be interpreted, however. It would appear that other potential safeguards cannot be read-in, for example: a search warrant power that might permit a search, but forbid access to electronic devices; or a warrant that limits the extent of the search that can take place in respect of those devices, so as to prevent the disclosure of irrelevant and sensitive material; or a warrant that required, where feasible, that electronic devices would be examined and copied *in situ*, so as to minimise disruption and interference with the privacy rights of the dwelling occupants.
62. Given the limitations of the section and the all-or-nothing nature of the decision whether to issue the search warrant, it is all the more important that there would be full disclosure of relevant facts so that the District Judge can make an informed decision.

### **Conclusion**

63. It is submitted that in the exercise of a warrant-issuer's discretion, a warrant may be refused on the basis that there was an intention to seize an electronic device but no proper justification was given for why that seizure was necessary.
64. If the warrant-issuer is not made aware of this intention however, they cannot properly or fairly exercise their discretion.

**Mark Lynam BL**