Searching for evidence in the digital age

Corporate Enforcement Authority Conference • October 19th 2023

Introduction

On November 11th 1762, Nathan Carrington, who bore the grandiose title of King's Chief Messenger, and three other King's messengers forcibly entered the home of John Entick in Stepney in East London. Over the course of four hours, they broke open locks and doors and searched all rooms in the house before taking away 100 charts and 100 pamphlets, causing £2,000 of damage (equivalent to c. €350,000).

Entick was a Grub Street hack with a fake master's degree. He was a staff writer in an anti-ministerial periodical called *The Monitor or British Freeholder*. *The Monitor* published essays and opinion pieces. Its controversialist tone wasn't to everyone's liking. A 1759 review colourfully described its contents as follows:

"*They are like middling sermons pronounced by a phlegmatic preacher, plain, heavy, and soporiferous; they co-operate with the narcotic steams of coffee, towards an afternoon's nap: they furnish the city-clubs with political chit-chat, serve to light pipes in the evening, and may be comfortably applied to another domestic purpose in the morning*."[1]

The King's messengers were acting on the orders of the Earl of Halifax who was then the newly appointed Secretary of State for the Northern Department (roughly equivalent to the Foreign Secretary). Halifax himself issued a warrant to search for Entick and "…*to seize and apprehend and bring together with his books and papers in safe custody, before the Earl of Halifax to be examined concerning the premises, and further dealt with according to law*".[2]

Entick sued Carrington for trespass in what became a landmark case in the delineation of the scope of executive power. Entick complained that the King's messengers "*read over*", "*pried into*", and "*examined*" all his papers, and without any regard to the potential relevance to the investigation, then carried them away, removing a vast amount of material and property, and causing Entick substantial pecuniary damage.

The case was tried by the Lord Chief Justice a jury in the Court of Common Pleas sitting in Westminster Hall. The jury returned a special verdict assessing damages in the event of a finding of liability. Lord Camden C.J. found that the warrant was void and the actions of the defendants a trespass. The court rejected a suggestion that the warrant was governed by the Constables Protection Act 1750 (which related to judicial warrants). The court posed the following rhetorical question in exchanges with counsel:

> "[S]*uppose a justice of peace issues a warrant to search a house for stolen goods, and directs it to four of his servants, who search and find no stolen goods, but seize all the books and papers of the owners of the house, whether in such a case would the justice of peace, his officers or servants, be within the* [1750 Act]*?*"[3]

[1] 'The Monitor, or British Freeholder' *The Critical Review, Or, Annals of Literature*. London: A. Hamilton. 7: 22–23. January 1759.
[2] *Entick v Carrington* (1765) 2 Wils. K.B. 275; [1765] 1 WLUK 1; 95 E.R. 807, at p. 808, § 276.
[3] *ibid.*, at p. 814, § 286.

This case long predates the advent of digital storage of information but addresses a central and perennial question about the extent to which searches for criminal material can encroach upon a citizen's right to privacy and legal professional privilege.

Searching for computers

In *People (DPP) v Quirke*,[4] the defendant was prosecuted for the murder of a man whose remains were found in a tank on the defendant's farm. Gardaí were granted a warrant to search his home. Among the items seized was his personal computer. An analysis of the computer revealed online searches said in relation to the decomposition of human remains. This provided a significant strand in the circumstantial case which led to Mr Quirke's conviction.

The warrant was issued under s. 10 of the Criminal Law Act 1997 (as amended by s. 6 of the Criminal Justice Act 2006). In applying for the warrant, gardaí made no mention of the fact that they desired, among other things, to seize and analyse his computer. The Supreme Court held that although the search was lawful, in the absence of specific permission being sought and given to search the computers, the search of the computer was not lawful.

The Supreme Court quoted the following passage of Roberts C.J. in the US Supreme Court case of *Riley v California*,[5] which underlined the significance of a cell phone as a repository of information. Charleton J. went on to hold that a computer is not a 'place' as defined in s. 10(6):

> "*It is, instead, a repository and recording of vast stores of information, beyond the capacity of even some public libraries, of the deeds, thoughts, obsessions and activities of a person, of the persons communicating with that person and of what is stored outside the computer on servers, on cached sites by service providers and more widely on the utilization of multiple computers through the cloud.*"[6]

Charleton J said that where a warrant permits the search of the place, it permits the seizure and analysis of a computer as a physical object. However, if the gardaí wish to analysis the contents of the computer as a portal into the digital world, this must be explicitly adverted to in the application for a warrant:

> "*97. A computer or other digital device must of necessity be found in a place but the seizure of it for testing involves the entry into the digital space and departure from the physical location seizure powers authorised by the 2006 Act. This difference necessarily requires authorisation for the search of the digital space outside the physical location enabled by the statutory power. When, in contrast to this case, a judge is told that computer devices, which includes mobile phones and akin digital instruments, are to be searched for and potentially seized, the judicial mind is entitled to infer that the purpose of search is to enable entry into the non-physical space controlled by the accused or to be found within the physical location to be searched. That search may be justified by appropriate information in the sworn information accompanying an application for a warrant. But the lawful search for and seizure of a computer requires judicial intervention on the settled authority of* Damache.[7] *The seizure for entry into the digital space involves the automatic loss of privacy rights on a vast scale. Without judicial scrutiny, seizure for the purpose of a non-physical search into mobile phones and other*

[4] *People (DPP) v Quirke* [2023] IESC 5 [2023] 1 I.L.R.M. 225.
[5] *Riley v California* 573 U.S. 373 (2014).
[6] *People (DPP) v Quirke* [2023] IESC 5 [2023] 1 I.L.R.M. 225, at § 96.
[7] *Damache v DPP* [2012] IESC 11; [2012] 2 I.R. 266; [2012] 2 I.L.R.M. 153.

> *computer devices of vast memory and carrying the private dimensions of a human life over years or months no balancing of rights can be undertaken whereby a court may authorise such a search and seizure.*"[8]

In *Quirke*, it was noteworthy that s. 10 warrants did not explicitly allow for the search and seizure of computers, unlike for example warrants issued under the Criminal Justice (Theft and Fraud Offences) Act 2001.

Computers and privacy rights

In *CRH v Computer and Consumer Protection Commission*,[9] the Competition and Consumer Protection Commission (CCPC) carried out and investigation into alleged anticompetitive practises in Irish Cement. A CPCC officer was issued a warrant under s. 37 of the Competition and Consumer Protection Act 2014 to search the premises of Irish Cement.

The warrant was executed and among the items seized was the email account of Séamus Lynch, then a former managing director of Irish Cement. The email account contained over 100,000 emails. During the search, negotiations were ongoing between the CPCC and Irish Cement in relation to the emails. It was agreed that the items would be seized but not gone through until an agreement was reached between them on a process by which this could be done.

Proceedings were ultimately brought by both Mr Lynch and Irish Cement. They complained that most of the 100,000 emails were private and outside the scope of the warrant. Therefore, they argued, the search and seizure were in breach of privacy rights protected by the Constitution and the European Convention on Human Rights. In the High Court Barrett J agreed and held the warrant did not authorise the seizure of certain materials and restrained the respondents from accessing certain of the material seized.

The defendants appealed. The Supreme Court noted that the right to privacy required that the contents of the items sized be scrutinised. This required the searched party to be able to ensure that the material was reviewed to prevent irrelevant material being seized. The court disagreed with the High Court and held that material could be lawfully removed from the premises under the warrant provided the review mechanism was in place.

In his judgment, MacMenamin J referred to *Entick v Carrington* and observed as follows:

> "*The constitutional and ECHR right to privacy is of central importance in the digital age in which we now live. The Charter of Fundamental Rights of the European Union …contains protection for private and family life and personal data (articles 7 and 8). It so happens that the allegations here concern what is called 'white collar crime'. Large companies such as ICL and CRH do not easily attract public sympathy. They make vast sums of money and make some people very wealthy. But, just as in* Entick v Carrington,[10] *the issue here is, precisely, whether the CCPC officers can rely 'on the words of the statute' in intruding upon the plaintiffs' rights to privacy in this way. These questions are to be tested now, by resort to proportionality, and against the protections*

[8] *People (DPP) v Quirke* [2023] IESC 5 [2023] 1 I.L.R.M. 225, at § 97.
[9] *CRH v Computer and Consumer Protection Commission* [2017] IESC 34; [2018] 1 I.R. 521.
[10] *Entick v Carrington* (1765) 2 Wils. K.B. 275; [1765] 1 WLUK 1; 95 E.R. 807.

> *of the Constitution and article 8 ECHR. The financial circumstances or social status of the plaintiffs are not a relevant consideration.*"[11]

The Supreme Court therefore restrained the CPCC from accessing the documents until an agreement was reached on the determination of privacy issues.

Searching computers and privilege

In *Corcoran v the Commissioner of An Garda Síochána*,[12] the applicant was a journalist with a small local newspaper. He received a tip off from a source and attended a scene in Strokestown where 20-30 people attended a bank eviction wearing balaclavas and armed with weapons. Security guards were assaulted and falsely imprisoned. Sentences were subsequently handed down of 15 years to some of the protagonists.

Three days later, Corcoran was interviewed under caution. He agreed to make the videos and images available but declined to reveal his sources citing journalistic privilege. Four months later, the District Court issued warrants under s. 10 of the 1997 Act to search Corcoran's home and the newspaper premises. The District Court was told that there may be videos and images on his phone which might assist in their investigation. The court was not told Corcoran was a journalist and had asserted privilege over his sources in interview and had indicated a willingness to share videos with gardaí.

The warrant was executed, and the phone handed over under protest. Judicial review proceedings immediately issued seeking to quash the warrant and seeking to compel the return of the phone. The case made its way to the Supreme Court. Hogan and Collins JJ both delivered judgments noting the lack of any provision in s. 10 of the 1997 Act to deal with privilege. The court noted that the choice of the District Court is binary: to issue the warrant or not. There is no provision in s. 10 for issuing it subject to conditions or limitations or subsequent review.

The court therefore read into s. 10 a requirement to put full information before the court. Hogan J noted *Quirke* and noted the privacy said to inhere in mobile phones.

> "*If this is so, then it is clear that the Oireachtas intended that the District Judge should, at least, in general terms, have all material information regarding the mobile telephone before him or her before the appropriate decision was made whether or not to issue the warrant. The fact that the owner of the mobile device was a journalist who had asserted journalist privilege was an absolutely critical detail, precisely because knowledge of this particular factor might well have caused the judge to refuse to issue the warrant for reasons I shall now seek to explain. It is true that the present appeal has exposed clear weaknesses in the operability and general workability of s. 10 of the 1997 Act (a topic addressed elsewhere in this judgment). Yet even as it stands it would have been open to the District Judge to refuse to issue the warrant had these facts pertaining to the issue of journalistic privilege been disclosed to him. This is because the very grant*

[11] *CRH v Computer and Consumer Protection Commission* [2017] IESC 34; [2018] 1 I.R. 521, at p. 543, § 38. By contrast, see the Hong Kong decision of *To Man Choy Jacky v Securities And Futures Commission And Another* [2020] HKCFI 270.

[12] *Emmett Corcoran and Oncor Ventures Ltd t/a The Democrat v Commissioner of an Garda Síochána and the Director of Public Prosecutions* [2023] IESC 15.

of the warrant might well have amounted to a breach of Article 10 ECHR and, to my mind, Article 40.6.1° of the Constitution as well."[13]

The warrant was quashed because the District Court was not told that the applicant was a journalist who had asserted privilege which might have led the court to refuse to issue the warrant in the absence of any safeguards or review in s. 10.

Statutory procedures dealing with privilege

Section 10 of 1997 Act contains no mechanism to deal with issues of privilege. However, some sections (*e.g.*, s. 48(6) of the Criminal Justice (Theft and Fraud Offences) Act 2001; s. 17A of the Sea Fisheries and Maritime Jurisdiction Act 2006; s. 64 of the Criminal Justice Act 1984) explicitly provide that items may be seized "*other than items subject to legal privilege*". This has the difficulty identified in *CRH* that the privileged items cannot be seized so privilege must be determined in situ.

Other statutory provisions (*e.g.*, s. 33 of the Competition and Consumer Protection Act 2014; s. 795 of the Companies Act 2014) provide for mechanisms for dealing with assertion of legal professional privilege in relation to items seized. They provide for the retention of the items seized in a confidential manner pending the determination of privilege by a court.

In *CEA v FAI & Delaney*,[14] gardaí seconded to the Office of the Director of Corporate Enforcement (now the CEA) searched the premises of the FAI on foot of a warrant issued by the District Court under the Companies Act 2014. Items were seized including the work email folder of John Delaney, the former CEO of FAI. As required by the 2014 Act, the ODCE immediately applied to the High Court seeking a determination on whether the items seized were privileged. Mr Delaney was made a notice party.

An examination strategy identified 285,000 files. Mr Delaney's solicitor (who was subsequently assisted by an IT expert) spent in the region of six months in the offices of the ODCE examining the material. He identified 29,500 documents which potentially attracted privilege. The court appointed a barrister (as provided for in the legislation) to look at the documents and report to the court. The barrister was given a 'context letter' by Delaney's solicitor which was not given to the ODCE. A second barrister was appointed in the teeth of objections from Mr Delaney. Ultimately a report emanated from them, identifying 1,123 documents which potentially attracted privilege.

Following the report, the High Court allowed further time for Mr Delaney to inspect the documents to enable him to put forward claims of privilege to allow the court to make the determination. The context letter was then disclosed to the ODCE who complained that it comprised in part a legal submission which they could not reply to before the report was made and which contained manifest errors.

The matter came on for hearing. Various claims of privilege were made over the documents under the heading of legal advice privilege and litigation privilege. The ODCE argued that Mr Delaney bore a burden of proof to demonstrate the privilege existed and that had not been discharged in relation to any of the documents of 1,123 referred to in the report. The High Court

[13] *Emmett Corcoran and Oncor Ventures Ltd t/a The Democrat v Commissioner of an Garda Síochána and the Director of Public Prosecutions* [2023] IESC 15, at §§ 98-99

[14] *Corporate Enforcement Authority v Cumann Peile na hÉireann 'Football Association of Ireland' and John Delaney* [2023] IECA 226.

agreed and declined to hold any privilege existed at all describing the assertions of privilege as "*vague and nebulous claims which are wholly unsubstantiated*".

Mr Delaney appealed to the Court of Appeal. The primary thrust of the appeal was that the High Court had rejected the assessors report in its entirety without giving reasons. The court was happy to infer from the course of the proceedings before the High Court that the assessors report was tainted by the context letter to which the ODCE did not have an opportunity to consider.

An issue arising in the appeal was a suggested necessity of the court to look at the documents to determine privilege. Mr Delaney relied on authorities in relation to public interest privilege where this exercise is often carried out. The ODCE successfully argued that for the vast majority of documents, the High Court was justified to decline to do so. Unlike public interest privilege, with LPP (in particular litigation privilege) looking at a document will not assist the court in determining whether it attracts privilege. The wider context is required but, according to the High Court, it was simply not provided.

Another issue that arose for consideration was the process of determining privilege. The court considered various authorities in relation to the determination of privilege and the burden of proof. However, in those cases there is a set of pleadings where the issues are defined. By contrast, in the process here, there are no pleadings and the ODCE had no context to put the material in (other than terse references made by Mr Delaney).

Conclusions

It seems clear that the State or its agencies cannot seize and analyse a computer or other device unless explicitly authorised to do so under a warrant. In doing so they may face issues of privilege and/or privacy. Depending on the statutory procedure invoked, there may or may not be an explicit mechanism to determine the issue by way of application to court or otherwise.

Although some statutes provide for dealing with legal professional privilege, there appears to be no statutory mechanism to deal with other forms of privilege, such as journalistic privilege. None of the statutory warrant procedures provide for a mechanism for the determination of relevance and privacy.

Examining the 1,000 pamphlets of Mr Entick for privilege or privacy might provide little difficulty. However, engaging with the work email folder of a former company officer or the work emails of a former Secretary of State and US presidential candidate is a vast undertaking as the procedural history of *Delaney* demonstrates.

It is not difficult to imagine an investigation that would involve multiple email folders and vast arrays of data which would dwarf those in *Delaney*. It is not clear how such investigations could ever be manageable for investigators or could be engaged with by defendants who may not have the means to employ a solicitor to sit in an investigator's office for six months.

It may be that the answer lies in technology to interrogate large amounts of data to consider issues of privilege, privacy and relevance having been instructed on the potential issues involved by the investigator. This, combined with a better designed statutory framework has the capacity to make these investigations manageable.

James Dwyer SC
October 15th 2023