Hard Data: Disclosure in the 21st Century

James Dwyer SC • 23rd Annual National Prosecutors' Conference

Introduction

This paper attempts to identify some of the legal and practical issues confronting prosecutors when making disclosure in modern criminal litigation. Historically the right of an accused to obtain disclosure of the case against him and to peruse the fruits of the investigation began to emerge as an issue in the nineteenth century.

In 1834 the British House of Commons debated the Counsel for Prisoners Bill which when enacted, gave an accused a right to be represented by counsel when tried for a felony. An amendment to the bill was proposed by the MP for Drogheda, Andrew O'Dwyer, which provided a statutory right to an accused to obtain a copy of depositions sworn against him in a committal hearing on which the indictment had been grounded.

The MP for Southern Wiltshire, John Bennett, was of the view this was unnecessary as, he suggested, depositions were routinely taken at committal hearings in the presence of the accused. According to Hansard, the MP for Dublin City, a practising barrister by the name of Daniel O'Connell observed that he:

> "*…was glad to hear that such was the case in England. He could assure the House the practice was diametrically opposite in Ireland, for there the prisoner knew nothing of the charge to be brought against him but the short abstract contained in the commitment, and it not unfrequently happened, that depositions taken on a subsequent charge were exhibited against him*."[1]

The amendment was withdrawn but subsequently reinserted by the House of Lords. The Duke of Richmond (who had served in the Peninsular War), expressed his opinion that the practice of taking depositions against a prisoner in his absence "*was more fitted for the meridian of Spain than to that of this free country*".[2] Indeed.

The amendment eventually came into force but did not entitle an accused to copies of depositions taken after the committal.[3] This led to prosecutors being accused of 'holding back' depositions being taken until after the committal hearing so as to prevent an accused getting access to them. All of this is a far cry from the service of books of evidence and notices of additional evidence under the Criminal Procedure Act 1967.

Legislating for disclosure

In December 2014, the Law Reform Commission published a detailed report on Disclosure and Discovery in Criminal Cases.[4] The report was created following submissions received from a broad array of contributors and includes a detailed analysis of the various issues involved and the competing interests at stake. A draft bill was appended to the report which attempted to introduce a comprehensive statutory framework for disclosure which addressed a range of conflicting rights. The report was

[1] HC Deb 03 July 1834 Vol. 24 Col. 1099.
[2] HL Deb 15 July 1836 Vol. 35 Col. 232.
[3] Section 3 of the Counsel for Prisoners Act 1836 (also referred to as the Trials for Felony Act 1836) 6 & 7 Will. 4 c. 114.
[4] LRC 112-2014.

launched to mixed reviews. Most notably the then DPP, Clare Loftus, expressed significant reservations in her address at its launch.

Rather than enact the draft bill as proposed, the Oireachtas in February 2017 promulgated s. 39 of the Criminal Law (Sexual Offences) Act 2017 which inserted a new section 19A into the Criminal Evidence Act 1992. This created a protocol for the disclosure of counselling records in sexual cases in the hands of non-parties. A number of problems can be identified with s. 19A:

1. The section only applies to sexual offences as appear in the schedule to the Sex Offenders Act 2001. Thus, for example in prosecutions for harassment or assault, counselling records cannot be obtained under this section, although there appears little basis to differentiate such prosecutions on that basis.

2. The section only applies to counselling records. A 'counselling record' is defined in s. 19A(1) as follows:

   > "*any record, or part of a record, made by any means, by a competent person in connection with the provision of counselling to a person in respect of whom a sexual offence is alleged to have been committed ('the complainant'), which the prosecutor has had sight of, or about which the prosecutor has knowledge, and in relation to which there is a reasonable expectation of privacy*"

   'Competent person' is defined as "*a person who has undertaken training or study or has experience relevant to the process of counselling*". Thus, only records created by a competent person fall within the section. So, if a family member provides counselling to a complainant, any notes he or she makes would not fall within the ambit of the section unless they had relevant experience or had undertaken relevant training.

3. The section only applies to cases before the Circuit Criminal Court or Central Criminal Court. The District Court and Special Criminal Court are excluded from the definition of 'court' under s. 19A(1). This might make a defendant less likely to elect for summary trial of a sexual assault offence where he would have fewer rights to disclosure.

4. The section provides on a plain reading that no disclosure can be made in any prosecution without leave of the court. The court is defined only as including the Circuit or Central. Therefore, in a trial before the District Court or Special Criminal Court, counselling records arguably cannot be disclosed, and the trial court cannot direct their disclosure.

5. Under s. 19A(17), the section is said not to apply when the complainant consents to disclosure. Therefore, if the complainant consents but the counsellor does not, the mechanics of the section are not available, and the court must fall back on its common law powers of subpoena in the face of the dicta of the Supreme Court in *JF v DPP*[5] which prohibited the use of subpoenas as a disclosure device.

[5] [2008] 1 I.R. 753.

6. The section provides for a role for the defence in making submissions in a disclosure hearing. This is done where the defence is unaware of the contents of the documents and its potential relevance. There is no provision in Irish law for the appointment of special counsel to argue the defence position having had sight of the documents.

7. The accused cannot appeal against a decision against him in a disclosure hearing. It appears his only remedy is to seek prohibition. This involves convincing the High Court that the absence of the material creates an unavoidable risk that his trial will be unfair as a result of the ruling.

8. The prosecutor has no right of appeal against a disclosure order either. If the court makes an order which is too wide in its scope, the prosecutor has no remedy (as it will be a decision within jurisdiction). The only potential remedy is to take the radical step of withdrawing the case.

Many of these issues have yet to arise in the four years since the section came into force.

The EU Disclosure Directive

The European Union has entered the arena of criminal disclosure by means of the Disclosure Directive.[6] This directive was made in May 2012 and was required to be implemented into domestic law by June 2nd 2014. This did not happen and the DPP conceded before the Supreme Court that the Disclosure Directive is directly effective in *People (DPP) v O'Sullivan*.[7]

The Disclosure Directive relates to rights to disclosure both of people incarcerated and people prosecuted. Article 7.2 describes a right of access to the materials in a criminal case:

> "*2. Member States shall ensure that access is granted at least to all material evidence in the possession of the competent authorities, whether for or against suspects or accused persons, to those persons or their lawyers in order to safeguard the fairness of the proceedings and to prepare the defence.*"

Article 7.3 provides that disclosure is to be made in a timely fashion:

> "*3. Without prejudice to paragraph 1, access to the materials referred to in paragraph 2 shall be granted in due time to allow the effective exercise of the rights of the defence and at the latest upon submission of the merits of the accusation to the judgment of a court. Where further material evidence comes into the possession of the competent authorities, access shall be granted to it in due time to allow for it to be considered.*"

Article 7.4 provides that disclosure can be refused in circumstances where it seriously impinges upon others provided the right to a fair trial is not prejudiced:

[6] Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings.
[7] [2018] IESC 15, at para. 15.

> "*4. By way of derogation from paragraphs 2 and 3, provided that this does not prejudice the right to a fair trial, access to certain materials may be refused if such access may lead to a serious threat to the life or the fundamental rights of another person or if such refusal is strictly necessary to safeguard an important public interest, such as in cases where access could prejudice an ongoing investigation or seriously harm the national security of the Member State in which the criminal proceedings are instituted. Member States shall ensure that, in accordance with procedures in national law, a decision to refuse access to certain materials in accordance with this paragraph is taken by a judicial authority or is at least subject to judicial review.*"

The Disclosure Directive appears yet to be litigated in the Superior Courts the context of a right to disclosure in a criminal trial. Article 7.1 was litigated in the context of the right to information of an accused while in custody prior to interview. In *Maloney v Member in Charge of Finglas Garda Station*,[8] Noonan J. held the application moot but noted the right of an accused to seek to consult with his solicitor mid-interview.

The Disclosure Directive appears to require a re-visiting of the vexed question of courts making disclosure orders against State non-parties.[9] It seems to empower a trial court to direct 'competent authorities' to make disclosure in a case to which they are not a party. For example, the Disclosure Directive might empower a trial court to make an order against the gardaí in a private prosecution or against Túsla in a DPP prosecution. The current protocols between the DPP and other State parties have meant this issue has not arisen.

Also, it is worthy of note that s. 3(1) of the European Convention on Human Rights Act 2003 obliges organs of the State to carry out their functions in a manner compatible with State's obligations under the convention, including presumably, Article 6.

The Disclosure Directive also does not explicitly provide that material disclosed would also be disclosed to the prosecution. Under current protocols material in the hands of Túsla or GSOC is transmitted to the accused via the prosecutor. An order made under Article 7.2 may not require this. However arguably transmission to the prosecutor as well as the defence would be required under Article 7.2 in order to "*safeguard the fairness of the proceedings*".

Data Protection law

The Data Protection Act 2018 implements into Irish law two pieces of EU legislation: the General Data Protection Regulation (GDPR)[10] and the Law Enforcement Directive (LED).[11] The GDPR governs the processing of data generally. The LED governs the processing of data by law enforcement authorities. For example, if a garda asks a

[8] [2017] IEHC 279.

[9] See the judgment of Edwards J. in *HSE v White* [2009] IEHC 242.

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[11] Directive (EU) 2016/680/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

shopkeeper asks for CCTV as part of an investigation, it is processed by the shopkeeper under the GDPR and by the gardaí under the LED.

Article 1.1 of the LED sets out the parameters of the directive:

> "*1. This Directive lays down the rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security*."

Article 8.1 of the LED provides for lawfulness of processing

> "*1. Member States shall provide for processing to be lawful only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) and that it is based on Union or Member State law*."

. Section 41 of the 2018 Act provides as follows:

> "*41. …the processing of personal data and special categories of personal data for a purpose other than the purpose for which the data has been collected shall be lawful to the extent that such processing is necessary and proportionate for the purposes…of preventing, detecting, investigating or prosecuting criminal offences…*"

Part 5 of the 2018 Act makes detailed provision for the implementation of the LED. Section 71(2) provides that the processing of data shall be lawful where and to the extent that "*the processing is necessary for the performance of a function of a controller for a purpose specified in section 70 (1)(a) and the function has a legal basis in the law of the European Union or the law of the State*".

Section 70(1)(a) of the 2018 Act describes data processed for the purpose of the prevention, investigation, detection, or prosecution of criminal offences, including the safeguarding against, and the prevention of, threats to public security, or the execution of criminal penalties. Under 71(5) the processing must be necessary and proportionate.

Section 73 provides for the processing of a special category of personal data. This is defined in s. 69 as including data relating to ethnicity, political opinions, trade union membership, genetics, biometrics, health, and sexual orientation. Section 73(1) provides for a variety of circumstances in which it is permissible to process special category data including under s. 73(1)(b)(v) where the processing:

> "*(I) is required for the purposes of providing or obtaining legal advice or for the purposes of, or in connection with, legal claims, prospective legal claims, legal proceedings or prospective legal proceedings, or*
>
> *(II) is otherwise required for the purposes of establishing, exercising or defending legal rights*;"

Notwithstanding the elaborate procedures in the 2018 Act, its implications for the duty on prosecutors to disclose appears limited. In essence the legislative framework allows for disclosure to take place as disclosure is a necessary function carried out by prosecutors. The requirement in 2018 Act that the disclosure made is necessary and proportionate is perhaps no more than the common law has provided for in any event.

Sex cases and phones

The proliferation of mobile phones and social media has dramatically increased the volume of material to be considered for disclosure. The capacity of such material to be relevant comes into sharp focus in case involving allegations of rape and sexual assault. For example, communications by a complainant in the early aftermath of an incident can be highly relevant.

The point is well illustrated by *DSK v R.*[12] There the appellant was convicted of rape. He admitted intercourse with the complainant but said it was consensual. The jury had been shown Facebook messages between the appellant and the complainant obtained from her. She said she deleted some messages between them to save space. The complainant asserted that after the intercourse, they only had limited contact which related primarily to her taking contraception.

Following his conviction, the appellant's sister downloaded the messages from his Facebook account. This showed that the complainant had selectively deleted messages exchanged between them after the alleged rape. It showed a large amount of contact between them. For example, his message 'sorry' was revealed to be a response from her suggesting he was ignoring her, not an apology for something that had happened. She had also deleted a message texting him her phone number (which he had lost) and adding kisses to the message. The conviction was quashed, and no retrial was sought.

On the other hand, the privacy rights enjoyed by an injured party need to be at the forefront. As Birmingham P observed in *People (DPP) v Robert Keogh*,[13] "*Simply because a person makes a complaint that they have been a victim of crime does not mean that they abandon their right to privacy or that they lose that right*."

An example of this in practice is given by the recent decision of *People (DPP) v Opoku*.[14] The appellant had raped the complainant in his home after meeting on a night out. They had not met before. Videos from her phone of the night were played to the jury showing her in an intoxicated state. He admitted sex but said it was consensual. Her phone was obtained, and portions of its contents were disclosed. The Court of Appeal rejected an argument that the conviction was unsafe due to lack of disclosure, commenting as follows:

> "*Phones are likely to contain records of very private material. In this case, it appears that 13,000 pages of material spilled over approximately one year. The prosecution approach of providing all material for a week prior to the incident and Tinder messages for one month prior to the incident was a very realistic one. Indeed, in a situation where nobody was suggesting that there had ever been any prior contact between the two accused and the two young women, it*

[12] [2017] EWCA Crim 2214. My thanks to Jane McGowan BL for informing me of this case.
[13] [2017] IECA 232, at para. 15.
[14] [2022] IECA 61.

> *might be said that, if anything, the prosecution was erring on the side of over-disclosure. Again, it appears that issues which were identified as potentially being of interest to the defence, such as attitudes and approaches to sex, references to ethnicity of individuals, and so on, were isolated and disclosed.*"[15]

The colossal volume of data produced by mobile phones demonstrates the real risk for such issues to arise. Data are often downloaded by software such as XRY and Cellebrite and can run to tens of thousands of pages. This then has to be considered by the prosecutor to determine what portions of it are required to be disclosed. This must be done in the absence of knowing what defence is being run by the accused.

The increasing practice of engaging documentary junior counsel to interrogate the large arrays of data has to date been used as a way of dealing with the issue. A longer-term solution may involve better software which interrogates the data in a way which allows for its perusal as if perusing the messaging apps on the phone itself. This could dramatically shorten the process of analysing vast quantities of data.

Conclusion

The advent of European law and modern technology presents challenges to prosecutors in ensuring an accused receives a fair trial while having due regard to the privacy rights of victims. It may be that advances in technology are the key to avoiding being drowned in vast quantities of data. What Daniel O'Connell would have made of it all is anyone's guess.

James Dwyer SC
November 16th 2022

[15] *ibid.*, at para. 20.