THE COURT OF APPEAL

The President
Edwards J.
Kennedy J

Record No: 26/18

BETWEEN/

THE PEOPLE AT THE SUIT OF

THE DIRECTOR OF PUBLIC PROSECUTIONS

Respondent

V

EVE DOHERTY

Appellant

Judgment of the Court delivered on the 31st day of May 2019 by Mr. Justice Edwards.

Introduction
1. This is the appellant's appeal against her conviction by a jury on the 1st of August 2017 of a single count of harassment, contrary to s. 10 of the Non Fatal Offences Against the Person Act 1997 (the "Act of 1997"). The appellant was acquitted by the jury of two other counts on the same indictment each alleging the making of a false statement, contrary to s. 12 of the Criminal Law Act, 1976.

2. The appeal raises several novel legal issues, and a number of more routine legal issues.

3. The first novel issue concerns whether evidence comprising data gathered and retained by a telecommunications service provider within the State and provided to a Chief Superintendent of An Garda Siochana pursuant to a request made under s.6 (1) of the Communications (Retention of Data) Act 2011 (the "Act of 2011") should have been excluded as inadmissible at the appellant's trial in circumstances where Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 ("Directive 2006/24/EC"), which the Act of 2011 was enacted to partially transpose, was declared invalid by the Court of Justice of the European Union ("the CJEU") on the 8th of April 2014, in conjoined cases no's C-293/12, *Digital Rights Ireland Ltd v Minister for Communications and others* and C-594/12 *Landesregierung and others* ("*the Digital Rights* and *Landesregierung* cases"), as representing a wide ranging and particularly serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union ("the Charter") that was not actually limited to what was strictly necessary, and therefore unjustified.

4. A further novel issue raised concerns whether evidence which comprises data within the meaning of the Act of 2011, gathered and retained by a telecommunications service provider outside of the State, and indeed outside of the European Union, and ultimately obtained by An Garda Siochána pursuant to a mutual assistance request, or by other means lawful in the jurisdiction in which it was obtained, was properly admitted at the appellant's trial in this jurisdiction in support of the prosecution case.

5. Yet another novel issue concerns the correct interpretation of s. 10 of the Act of 1997, and in particular whether the types of behaviour listed in s.10(1) as potentially comprising the *actus reus* of the offence of harassment (subject to the establishment of persistence, and of the threshold level of harm identified in s. 10(2)) namely: "watching", "pestering" "besetting" or "communicating", are to be given their natural and ordinary meanings; or, alternatively, in some or all cases are to be given autonomous legal meanings such as, in the case of "watching" or "besetting", the meanings attributed to those words in s.7 of the Conspiracy and Protection of Property Act 1875.

6. The more routine issues, also raised, concern the adequacy of proof of the provenance of certain documents; the trial judge's failure to exclude evidence obtained in alleged breach of the right to privacy; the allegedly wrongful admission before the jury of certain evidence given by non experts which was alleged to be opinion evidence; alleged prejudice arising from the failure of the trial judge to grant directions on the two other counts on the indictment and of which the appellant was ultimately acquitted, and alleged failure by the trial judge to adequately address an issue arising from the closing address of counsel for the prosecution.

The Background to the Prosecution
7. At the time of the alleged offences, the complainant worked in the office of the Director of Public Prosecutions, and the appellant worked as a member of the gardaí.

8. The complainant gave evidence that in September 2011 she received a letter, purportedly authored by persons who were her neighbours. The letter was exhibited and although it contains no ink signature, is signed in typescript as being from "*The nice neighbours living in this area*". The complainant described it as a "*horrible letter*" containing "*insulting derogatory language*", and that it was "*vitriolic*". The terms of the document exhibited reveal that this characterization was not an understatement, laced as it was with profanity, insults and bile. It referred to the purported authors' delight at the complainant being absent from "*the road*" for two weeks while she was on holidays; it asserted that it was a widely held view that she considered herself "*far more superior than anyone else on the road*" just because she was "*a solicitor working for the state*"; it expressed pity for the complainant's child for having the complainant as a mother; and it alluded to the complainant's separation from her husband, offering the view that it didn't take her husband long "*to see sense*". The complainant told the jury that she was shocked and distressed on receiving this letter and that she had passed it on to the Gardaí.

9. In November 2011, a letter was sent to the then recently appointed Director of Public Prosecutions (DPP). It addressed the DPP by her first name and purported to "*warn her*" about the complainant. The letter referred to the complainant as a "*corrupt evil bitch*" and asserted incorrectly that she was niece of a named TD. The complainant is related to the named TD but much more distantly so than was suggested. She is a second cousin of the TD in question. The letter asserted that the complainant was destroying the DPP's name, that she was two- faced, that she had actively lobbied politicians to block the DPP's appointment, and that "*she will be nice to your face but will stab you in the back*". The letter was again not signed in ink, but bore a typed signature, namely that it was from "*A friend*". The envelope bore a Dublin Mails Centre postmark. The complainant told the jury that she had been very upset to learn of this letter, that there was no truth in its contents, that it was "*just rubbish*".

10. The complainant further testified that at the beginning of December 2011 a leaflet was distributed by placing it on cars in the large suburban estate where she lives. This estate includes a number of *cul de sacs* and the complainant lives in one of those. Although the leaflets in question were widely distributed throughout the estate, none were left in the *cul de sac* in which the complainant lives. However, she was telephoned by a neighbour who lived elsewhere in the estate, who had encountered one of the leaflets, and who felt the complainant should be made aware of it. Shortly afterwards, another neighbour, who had also found one of these leaflets, called to the complainant's door and hand handed the leaflet to her. The leaflet, which did not identify any real or purported author, named the complainant and characterized her as being "*dwarf*", "*two-faced*" and a "*bitch"*. As had the letter to the DPP, it again incorrectly asserted that she was the niece of a named TD. The leaflet had photographs, positioned side by side and above the accompanying text, of both the complainant and the named TD. It referred to the complainant as allowing members of a named family, "*her best friends*" to get "*off with drug dealing in the area*". The leaflet went on to state:

> "*We do not want drug dealers or corrupt State Solicitors living in our estate. Tell everyone that you know, including papers, radio, TV, about the corrupt politicians, Ms (*the complainant, explicitly named*) and the drug dealers (*the previously identified family, again explicitly named*), who are her best friends, that are living in our estate.*
>
> *POLITICAL CORRUPTION AND DRUG DEALERS IN (identified house numbers, one of which was the complainant's residence and the other of which was that resided in by the identified family).*
>
> *GET THEM OUT OF OUR ESTATE NOW BEFORE ONE OF OUR KIDS DIE AS A RESULT OF A DRUGS OVERDOSE!!!!!."*

11. The complainant told the jury that she had become aware that a neighbour's teenage son, a member of the named family, was involved in some trouble, but she had had no professional involvement whatever with the case. The boy had been found in possession of a small quantity of cannabis and was later charged with possession of a controlled drug contrary to s.3 of the Misuse of Drugs Act 1977. The case was dealt with in the District Court and he received the benefit of Probation Act. The complainant told the jury that the boy's mother, whom she did not think knew for whom she worked, rather merely that she was a solicitor, had telephoned her at home in some distress after their house had been searched by Gardaí. She stated that she told the mother where she worked, that in the circumstances she couldn't offer any advice, and suggested that she should seek legal advice elsewhere.

12. The jury further heard evidence that on the 31st of March 2012, at 13.40, an encrypted e-mail service known as 'hushmail' was used to send a lengthy disparaging e-mail concerning the complainant to numerous recipients. The email emanated from the address markkenny@hushmail.com. The subject line on the e-mail was in the terms: "*Corruption in the DPP's office*, (named TD)'s *niece Ms* (the complainant, explicitly named)." The e-mail alleged, *inter alia*, that the complainant was involved with her supposed uncle in political corruption. It suggested that the complainant "*makes sure her family and TD cronies never gets prosecuted*". It asserted that her "*best friends*", i.e., the identified family (again explicitly named) had been caught with a large amount of drugs and that she had made sure they were not prosecuted for it. It referred to her salary; it referred to her "*brand new silver jeep*" (the complainant had a silver Nissan Qashqai at the time); it alleged that she had received promotions and pay rises when others were getting pay deductions, and that she only worked a four-day week. It referred to her as being lazy and as rejecting 70% of all sex crime referrals and that "*the public need to know the truth*". It went on to assert "*I can tell you its down to TD's slotting their useless relatives into cosy positions, to look after them*"

13. One minute after the last emails were sent, at 13.41 on the 31st of March 2012, a further series of emails were sent from the same hushmail account, and again addressed to same numerous recipients, and with the same subject line as the previous email. Although the text of this message was slightly different to the previous one in terms of formatting, the wording of the document was identical to the previous one.

14. The jury further heard that on the 21st of April 2012 a letter was sent to the Office of the Director of Public Prosecutions, addressed to "To Whom It May Concern", making certain allegations about the complainant, this time incorrectly identifying her as being the sister of a TD, (the same named TD who was earlier suggested to be the complainant's uncle) and detailing allegations of corruption and nepotism, all of which are disputed and completely refuted by the complainant. It alleged that the complainant "*is the most useless person in the place and only got promoted because of her brother TD* (the previously named politician, again explicitly named."

15. On the 1st of June 2012, the 4th of August 2012 and the 16th of March 2013, further e-mails promulgating similar type allegations were again sent from a hushmail account to numerous recipients, including (amongst others) the POA (Prison Officers Association), the INTO (Irish National Teachers Organisation), the HSE, ESB Networks, the Rotunda Hospital, the editors of and/or journalists with two national newspapers, and the complainant's family doctor. On these occasions the emails emanated from sender accounts in the names of johngilligan@hushmail.com, clairefoley@hushmail.com, and brendanbarr@hushmail.com. As well as alleging the same type of nepotism and corruption as in previous e-mails, these e-mails suggested the complainant had received numerous undeserved promotions, and that work colleagues had taken civil actions against her, all of which were "*settled out of court to keep it quiet*". They referred alleged illegal fireworks parties at the complainant's home. They referred to "*luxury holidays*" allegedly taken by the complainant involving "*sunning herself in LA, Spain, France and London*" and going to luxury hotels in Ireland "*every weekend*". They alleged that the complainant has taken her son out of school on the pretext of being sick in order to accompany her on luxury holidays and to attend "*Arsenal matches*" but that she was not "*investigated or fined over it as other parents were*." They further alleged tax evasion, child neglect, allowing her 11-year-old son to have access to firearms, having drugs parties in her house and referred explicitly to the complainant as being "*deranged*" and "*incompetent*" and a "*useless hobbit*". The complainant emphatically refuted all of these allegations in her evidence. She told the jury that her taxes had been audited and that she had had no problems. She herself occasionally went Clay Pigeon shooting. However, she owned no firearms and her son had never been allowed access to firearms. Like many little boys he liked "Nerf" guns, which are toys, and she had brought him on one occasion to an "Airsoft" rifle range so that he could shoot at targets, but this was entirely legal.

16. The email of the 4th of August 2012 went so far as to allege that a brother of the complainant, who was a director of a diving company, had murdered one of the company's employees, a diver, and that the complainant "*made sure her brother was not*

prosecuted for murder" and "*had huge influence over the decision in the case*". The complainant in her evidence confirmed that there had been a fatal industrial accident involving an employee of a diving company of which her brother was a director. This had given rise to a health and safety prosecution of the company concerned. However, the complainant was not involved in any way in that case. In her evidence the complainant emphatically denied and rejected all allegations of wrongdoing or unprofessionalism.

17. Counsel for the appellant, in cross-examining the complainant, explicitly accepted that none of the allegations were justified, and that indeed they were defamatory, but put it to the complainant that the appellant was not the author of the e-mails and other documents in question.

18. The complainant gave evidence concerning the upsetting nature of the defamatory material that had been promulgated about her, and the inferences which she believed people would be likely to draw from the allegations. She stated:

> *"Well, it really upset me and really worried me. Some of the correspondence referred to my son, that just really worried me. I was in work all day and he was at home. I did have a childminder, but I just worried about him. It also -- I was just worried, I didn't know where it was coming from. There was a lot of personal information, so it made me feel that it was somebody who knew something about me. Some of the letters purported to be from my work colleagues, others from neighbours or I wondered if somebody had a grudge against me or whatever, so I just simply didn't know where it was coming from and that -- very distressed and very uneasy…"*
>
> *"I mean, it's very upsetting. It alleged that you're corrupt, you're politically appointed, you're lazy, you don't have the experience for the job, I mean, that's all extremely upsetting. It paints a picture of me as sort of this woman who just swans around, which is far from the truth. I live in a three-bedroomed semi-detached house. I have a very ordinary life, I work incredibly hard and my son is my priority, and that just gives a completely malicious and false impression of me…"*
>
> *"They made me very anxious. I stopped sleeping, I became nervous because I didn't know who was doing it but whoever did they seemed to know quite a lot about me. I know I became nervous at night, I wondered was somebody going to come to the house, I became anxious about my son, I was forever checking up that he was okay, on the road, out playing or whatever, checking up with Emma where he was, what he was doing, et cetera. I also lost my confidence which -- I don't know why. I think maybe when you've had such awful things said about you and published to so many people, just that was one of the effects it had on me, just undermined my confidence."*

19. It was clear from the evidence that some of the material included in the controversial documents could not have been known by a person who did not have some personal knowledge of the complainant. The appellant admitted at trial pursuant to s.22 of the Criminal Justice Act 1984, that at the time of the communications she was in a relationship with the complainant's ex-husband.

20. The jury heard evidence from several Gardaí and other witnesses called by the prosecution, to the effect that "hushmail" is the trading name of Hush Communications Canada Incorporated, an internet service provider based in Vancouver in Canada. The jury learned that the Minister for Justice and Equality in Ireland, as the Central Authority under the Criminal Justice (Mutual Assistance) Act, 2008, had submitted a mutual assistance request to the Government of Canada for records held by Hush Communications Canada Incorporated, at the behest of Gardaí investigating alleged harassment of the complainant. They further heard that on the 29th of July 2015, arising from this request for mutual assistance, an evidence-gathering order was obtained by Canadian police from the Honourable Associate Chief Justice Cullen of the Supreme Court of British Columbia. Having been apprised of the making of this order, Hush Communications Canada Incorporated recovered certain information from its records, namely IP and activity logs, relating to a number of hushmail accounts including markkenny@hushmail.com; johngilligan @hushmail.com; clairefoley@hushmail.com; michaelmullen@hushmail .com and brendanbarr@hushmail .com and this information was in due course furnished to An Garda Siochana via their Canadian counterparts. Two witnesses from "hushmail", namely Steven Olaf Youngman and Darryl Krassman testified before the jury concerning the nature of the information in question and the circumstances in which it was recovered and transmitted to the Gardaí. The jury learned from them that the controversial emails of the 31st of March 2012, the 1st of June 2012 and the 4th of August 2012 had all been sent from an account using an internet protocol (IP) address, namely 86.43.97.192, which was assigned to an Eircom customer. The emails sent on the 16th of March 2013 had been sent from an account using a different internet protocol (IP) address, namely 86.45.43.81, which was assigned to an Eircom Indigo customer. The jury further heard from Garda witnesses who had requested data retained by both Eircom and Eircom Indigo, respectively, pursuant to s.6(1) of the Communications (Retention of Data) Act 2011, and from a witness from Eircom and Eircom Indigo concerning the provision of this data to An Garda Siochana. Utilising this data, it was established by investigating Gardaí, and could be demonstrated to the jury, that in both cases the IP addresses in question were allocated to Y & T Infotech, an internet café trading as "Wired" at 15 Aungier St in Dublin 2.

21. The appellant accepted at trial by means of an admission made pursuant to s. 22 of Criminal Justice Act 1984 that she had been present in the said internet café on the 28th September 2013. The relevance of this was that an e-mail had been sent from this location at 12.03 on that date to numerous recipients making allegations about Martin Callinan who was the Garda Commissioner at that time. The said email had emanated from a sender account in the name of michaelmullen@hushmail.com.

22. The back ground to the discovery of this separate incident was that complainant had brought the publication of the defamatory e-mails and other documents concerning her, of which she had become aware, to the attention of An Garda Siochana at a relatively early stage, and the Gardaí had commenced an investigation. In the course of this investigation the Gardai came into possession of a photograph, which was in fact a still from a CCTV recording, and they regarded a woman in this photograph as being a person of interest in connection with their investigation. The investigating Gardaí, having already ascertained that the e-mails relating to the complainant had been sent from the aforementioned internet café, showed this photograph to the café's owner, a Mr Babu Kandru, and requested him to keep an eye out for the person in the photograph and to notify them if he encountered that person.

23. Mr Kandru testified before the jury that on the 28th of September 2013 the person in question came into his café and paid €2 to use the internet. She was directed to terminal no 15 and logged on there at 11.47 am.

24. About 15 minutes later a Garda, Detective Garda AR, came in to the shop, and Mr Kandru pointed out the person at terminal 15 to him as being the person in the photograph he had been shown.

25. Mr Kandru stated to the jury that he has the facility, as the operator of the café, to see what activity was taking place on each terminal in his premises. Primarily this was used to prevent underage persons from viewing inappropriate content. On this occasion he noted that the user at terminal 15 was logged on to an e-mail account and that she was using the e-mail address michaelmullen@hushmail.com and that the subject of the e-mail she was sending was entitled "Corrupt Garda Commissioner Needs Investigating Urgently". Mr Kandru had the presence of mind to note down these details, and also the email addresses of intended

recipients, on a piece of paper. .He then showed the screen of his operator's terminal, and what he had noted down, to Detective Garda AR, who used his mobile phone to record photographic screenshots from Mr Kandru's terminal.

26. Detective Garda AR then took up a position at terminal 11, close to terminal 15. He could see that the woman was logged in to what appeared to be an email account. He told the jury that the woman at terminal 15 was wearing a black beanie hat, had brown wavy hair, a black jacket, black trousers, brown sunglasses. As previously alluded to, it was admitted on behalf of the appellant that she was the person in question. It was established later in evidence that she was wearing a wig at the time, and the prosecution suggested that this and the wearing of the beanie hat and the sunglasses, was all in an error to disguise herself.

27. After some time, the woman logged off and she then left the internet café. She was observed doing so by Sergeant PC who told the jury that she was then followed by Gardai from Aungier Street, where the internet café was located, to an address in the suburbs of Dublin, which was the appellant's home address. It was by this means that the woman was identified as being the appellant.

28. After the appellant had left the internet café, Detective AR also left briefly but then returned and took possession of the hard drive, being the "C" drive, in the system unit at terminal 15, for later expert technical examination. There was evidence that it was discovered upon such technical examination that the appellant had, before leaving, "wiped" or erased all data from the said "C" drive. A few days later Detective AR also took possession of the notes that had been made by Mr Kandru.

29. The case against the appellant was based on circumstantial evidence. While there was no direct evidence to establish that she was the author and sender of any of the documents relied upon by the prosecution as containing material that formed part of a campaign of harassment directed at the complainant, there was very strong evidence to suggest that she had sent the e-mail to Commissioner Callinan. Comparisons were invited between all of the documents relied upon as harassing material directed at the complainant, and reliance was placed on features in common. In addition, as a central plank of their case, the prosecution sought to link the earlier emails concerning the complainant to the email sent about Commissioner Callinan. Comparisons were invited between, *inter alia*, certain recipients in common, the language used, the fact that that in all cases hushmail accounts had been used, and that in all cases the same internet café had been used. The jury were invited to draw an inference from the available evidence that the appellant had been the author and sender of the e-mail to Commissioner Callinan; and the further inference that she had also been the author and sender of the earlier e-mails, leaflets/posters and letters concerning the complainant. This further inference was invited on the basis of certain similarities as to modus operandi, particularly where e-mails were the vehicle by means of which the harassing material was promulgated, and in the case of all documents certain similarities in terms of the language used, the type of disparagement engaged in, the content in each case, and commonality of addressees/recipients in at least some cases.

30. The appellant was convicted by a jury of the harassment offence, and on the 19th of January, was sentenced to three years imprisonment backdated to the 30th of October 2017, the date on which she went into custody. She now appeals against both the conviction and sentence.

Grounds of Appeal

31. The appellant appeals against her conviction on sixteen grounds. These are:

> (i). The trial judge erred in law and in principle in failing to exclude evidence obtained under the Communications (Retention of Data) Act 2011;
>
> (ii). The trial judge erred in law and in principle in failing to exclude the evidence of Steven Olaf Youngman and Darryl Krassman in respect of data obtained from Canada;
>
> (iii). The trial judge erred in law and in principle in failing to discharge the jury in circumstances where the ruling made in respect of the application to exclude evidence obtained under the Communications (Retention of Data) Act 2011 referred to information/Directives which had not been opened to the court and on which no submission had been made;
>
> (iv). The trial judge erred in law and in principle in failing to exclude evidence of an email purportedly sent on the 28th September 2013 on the basis of an infringement of the right to privacy;
>
> (v). The trial judge erred in law and in principle in failing to exclude evidence of handwritten documents, for the purpose of comparison with other documents, in absence of evidence that those documents were written by the accused;
>
> (vi). The trial judge erred in law and in principle in failing to exclude evidence of typed documents found in the accused's home, for the purpose of comparison with other documents, in absence of evidence that those documents were written by her;
>
> (vii). The trial judge erred in law and in principle in failing to exclude evidence of typed documents found in the accused's locker, for the purpose of comparison with other documents, in absence of evidence that those documents were written by her;
>
> (viii). The trial judge erred in law and in principle in failing to exclude the evidence of Suzanne Lindsay and Sarah Skedd and in allowing copies of the presentations created by those witnesses to be given to the jury.
>
> (ix). The trial judge erred in law and in principle in failing to grant a direction on counts 2 and 3 (the two counts of making a false statement of which the appellant was acquitted by the jury).
>
> (x). The trial judge erred in law and in principle in failing to grant a direction on Count 1 (the sole count of harassment of which the appellant was ultimately convicted).
>
> (xi). The trial judge erred in law and in principle in finding that communications with third parties could constitute harassment.
>
> (xii). The trial judge erred in law and in principle in ruling that a letter sent to the office of the complainant and posters being displayed in her local area were capable of coming within the definition of "communicating with" for the purpose of a charge of harassment.
>
> (xiii). The trial judge erred in law and in principle in ruling that emails sent to third parties were capable of coming within the definition of "besetting" in the context of an offence of harassment.

(xiv). The trial judge erred in law and in principle in ruling that "to beset" was defined as "to trouble someone or something" in the context of the offence of harassment."

(xv). The trial judge erred in law and in principle in refusing to discharge the jury where prosecuting counsel in his closing speech placed emphasis on a document being found on a scanner with a separate header which had not been adduced in evidence, or any attention drawn to this during the evidence, to the court or to the defence, and the learned trial judge erred in law and in principle in telling the jury to ignore this aspect of the prosecution's closing speech;

(xvi). The trial judge erred in law and in principle in her charge to the jury in saying that to convict of the harassment that they did not need to be satisfied that the appellant had committed all the acts alleged.

32. For the purposes of the written submissions filed on her behalf, certain of these grounds were sensibly grouped together under broad headings on the basis that they were connected and inter-related. We propose to do likewise in addressing the issues raised.

Grounds (i), (ii) and (iii) – Retention of Data

33. An application was made in the absence of the jury to exclude evidence obtained under s. 6(1) of the Act of 2001 relating to subscriber details for the internet protocol (IP) addresses that were of interest, and to exclude the proposed evidence of the two Canadian witnesses alluded to earlier in this judgment, namely the witnesses from Hush Communications Canada Incorporated. These two pieces of evidence, when combined, had enabled Gardaí to ascertain that the email of the 28th of September 2013 relating to Commissioner Callanan had been sent from the "Wired" internet café; and evidence that that was so combined with the other evidence rehearsed earlier in this judgment, and in particular the eye witness evidence concerning what had occurred on the day in question, both at the "Wired" internet café and elsewhere, enabled a case to be mounted against the appellant on a circumstantial basis. The purpose of seeking to exclude these two pieces of evidence was to ensure that essential links in the circumstantial case were eliminated, with a view to effectively undermining that case.

34. Section 6(1) of the Act of 2001 provides:

> "A member of the Garda Síochána not below the rank of chief superintendent may request a service provider to disclose to that member data retained by the service provider in accordance with section 3 where that member is satisfied that the data are required for—
>
> (a) the prevention, detection, investigation or prosecution of a serious offence,
>
> (b) the safeguarding of the security of the State,
>
> (c) the saving of human life."

35. There was evidence on the *voir dire* that two s.6 (1) requests were made, namely one by Chief Superintendent John Gilligan on the 17th of August 2012, and one by Chief Superintendent Peter Kirwan on the 20th of March 2013. Both applications were granted. It was not suggested that there was a failure in either case to satisfy the statutory pre-conditions for the lawful making of such requests. Rather, the complaint was that the underlying statute, namely the Act of 2011, was itself in breach of European law and that it should, in effect, be disapplied by the trial court. The trial court was being asked to approach matters on the basis that there was in Ireland neither any lawful statutory power on foot of which data could be retained by a telecommunications service provider, nor, if retained, lawfully requested by and provided to a member of An Garda Siochana for the prevention, detection, investigation or prosecution of a serious offence or for any other purpose.

36. The case made before the court below, and again before us, is that the Act of 2011 has to be viewed as contrary to EU law in circumstances where it was enacted specifically with a view to partially transposing Directive 2006/24/EC which was declared invalid by the CJEU on the 8th of April 2014, in the *Digital Rights* and *Landesregierung* cases, and that the trial judge was obliged in the circumstances to disapply it.

Relevant legislative history and jurisprudence of the CJEU.

37. To appreciate fully all the nuances of the argument being made by the appellant it is necessary to have an overview of the relevant legislative history (particularly at EU level) and to understand the scheme of, and certain key provisions of, the principal instruments that require to be considered, as well as how jurisprudence arising from relevant litigation before the CJEU has influenced and affected how they must be interpreted.

38. At the time of preparation of this judgment data protection in the European Union is governed by Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 (otherwise known as the General Data Protection Regulation or GDPR) which came into force across the EU on the 25th of May 2018. Although nothing turns on it in terms of the issues that require to be addressed in this judgment, we simply observe that the GDPR is a directly applicable measure and did not generally require transposition into Irish law. The Oireachtas has, however, availed of the opportunity presented by the coming into effect of the GDPR to significantly modify our domestic data protection framework, which is now governed by the Data Protection Act 2018.

39. Be that as it may, what is important to appreciate in terms of the issues arising in this case is that the GDPR replaced a pre-existing European legislative framework on data protection comprising Directive 95/46/EC (commonly referred to as "the Data Protection Directive") which was substantially amended by Directive 2002/58/EC (commonly referred to as "the ePrivacy Directive"). Article 1(2) of Directive 2002/58/EC states that its provisions "particularise and complement" Directive 95/46/EC.

40. This pre-GDPR European legislative scheme was further complicated by the subsequent enactment of two more Directives which in turn amended Directive 2002/58/EC, namely Directive 2006/24/EC (commonly referred to as "the Data Retention Directive") which was later challenged and struck down as invalid by the CJEU in the *Digital Rights and Landesregierung* cases, and Directive 2009/136/EC (commonly referred to as "the Citizen's Rights Directive).

41. Unlike the GDPR, none of the instruments comprising the pre-existing European legislative framework on data protection was directly applicable. At the time of the enactment of Directive 95/46/EC Ireland already had domestic legislation governing data protection. This was the Data Protection Act, 1988 (the Act of 1988) which was enacted to give effect to the Strasbourg Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, a Council of Europe instrument which Ireland had signed on 18/12/1986 and was shortly to ratify (Ireland in fact ratified the Strasbourg Convention on 25th of April 1990). However, the Act of 1988 was not fully compliant with Directive 95/46/EC and required to be amended to achieve a full and effective

transposition of that measure. This led to the enactment of the Data Protection (Amendment) Act 2003, which was effective to transpose Directive 95/46/EC into Irish law.

42. Directives 2002/58/EC, 2006/24/EC and 2009/136/EC were subsequently collectively transposed by means of a combination of the Act of 2011 and the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations, 2011, S.I. 336/2011 ("the 2011 Regulations") (sometimes referred to as "the ePrivacy Regulations"). However, following the striking down of Directive 2006/24/EC in the the *Digital Rights and Landesregierung* cases, and the subsequent litigation before the CJEU in the *Tele2 Sverige and Watson* cases, there was uncertainty and doubt as to whether, and to what extent, the Act of 2011 and the 2011 Regulations, and the earlier related domestic legislation, remained EU law compliant. That uncertainty and doubt had not been resolved by the time that the entire code was replaced by the new legislative dispensation that is now the GDPR.

43. It is necessary at this point to briefly describe, to the extent relevant, some of the main features of the relevant EU Directives.

44. Directive 95/46/EC set up a regulatory framework which sought to strike a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the European Union. To do so, the Directive set strict limits on the collection and use of personal data and demanded that each Member State set up an independent national body responsible for the supervision of any activity linked to the processing of personal data.

45. Directive 95/46/EC was said in Article 3(2) thereof to apply to data processed by automated means (e.g. a computer database of customers) and data contained in or intended to be part of non-automated filing systems (traditional paper files). It did not apply to the processing of personal data:

- by a natural person during purely personal or household activities;

- during an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union, and in any case does not apply to processing operations concerning public security, defence, State security and the activities of the State in areas of criminal law.

46. "Personal data" was defined in Directive 95/46/EC as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

47. "Processing of personal data" was defined in Directive 95/46/EC as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction".

48. The Directive aimed to protect the rights and freedoms of persons with respect to the processing of personal data by laying down the key criteria for making processing lawful and the principles of data quality. Data processing was only lawful, per Article 7, if

- the data subject has unambiguously given his consent; or

- processing is necessary for the performance of a contract to which the data subject is party; or

- processing is necessary for compliance with a legal obligation to which the controller is subject; or

- processing is necessary to protect the vital interests of the data subject; or

- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party; or

- processing is necessary for the purposes of the legitimate interest pursued by the controller or by the third party, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection.

49. The principles of data quality, which must be implemented for all lawful data processing activities, were set out in Article 6 of Directive 95/46/EC. It provided that personal data must be processed fairly and lawfully, and collected for specified, explicit and legitimate purposes. They must also be adequate, relevant and not excessive; they must be accurate and, where necessary, kept up to date; and, *inter alia*, they must not be stored for longer than necessary and solely for the purposes for which they were collected.

50. Under Part V of Directive 95/46/EC, the person whose data are processed, the data subject, could exercise certain rights including: the right to obtain information being controlled or processed; a right of access to such data; a right to object, on legitimate grounds, to the processing of data relating to him/her; and a right to be informed before personal data was disclosed to third parties for the purposes of direct marketing, and to be expressly offered the right to object to such disclosures.

51. Directive 95/46/EC went on to provide, in Article 13 thereof, that Member States might adopt legislative measures to restrict the obligations and rights provided for:

> "when such a restriction constitutes a necessary measure to safeguard:
>
> (a) national security;
>
> (b) defence;
>
> (c) public security;
>
> (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
>
> (e) an important economic or financial interest of a Member State or of the European Union, including monetary,

budgetary and taxation matters;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others."

52. Other relevant provisions of Directive 95/46/EC related to the confidentiality and security of data processing; the notification of processing to a supervisory authority; judicial remedies, liability and sanctions; and the transfer of personal data to third countries.

53. As previously stated, Directive 95/46/EC was substantially amended by Directive 2002/58/EC. It explicitly recognised that information is exchanged through public electronic communication services such as the internet and mobile and landline telephony and via their accompanying networks. Directive 2002/58/EC set out rules to ensure security in the processing of personal data, the notification of personal data breaches, and confidentiality of communications. It required that providers of electronic communication services should secure their services by at least ensuring personal data are accessed by authorised persons only; by protecting personal data from being destroyed, lost or accidentally altered and from other unlawful or unauthorised forms of processing; and by ensuring the implementation of a security policy on the processing of personal data.

54. Directive 2002/58/2002 also required a service provider to inform the national authority of any personal data breach within 24 hours. If the personal data or privacy of a user was likely to be harmed, the user also had to be informed unless specifically identified technological measures had been taken to protect the data. Member States were further required to ensure the confidentiality of communications made over public networks, in particular: by prohibiting the listening, tapping, storage or any type of surveillance or interception of communications and traffic data without the consent of users, except if the person was legally authorised and in compliance with specific requirements; by guaranteeing that the storing of information or the access to information stored on user's personal equipment would only be permitted if the user had been clearly and fully informed, among other things, of the intended purpose and had been given the right of refusal; and by ensuring that when traffic data was no longer required for communication or billing, they should be erased or made anonymous. However, service providers might process these data for marketing purposes for as long as the users concerned were prepared to give their consent. This consent could be withdrawn at any time.

55. The Directive also banned unsolicited communications where the user had not given his/her consent. As amended by Directive 2009/136/EC (which is uncontroversial in the context of the present case) that ban was extended to so called "cookies" stored on users' computers or devices.

56. Of relevance to the issues in the present case is Article 15(1) of this Directive, which provided:

"Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union."

57. Moving then to Directive 2006/24/EC, the background to the enactment of this, later impugned, instrument, which sought to amend Directive 2002/58/EC, is to be found in the preliminary recitals thereto, the most relevant of which were quoted in paragraphs 12 to 15 inclusive of the judgment of the CJEU in the *Digital Rights and Landesregierung* cases, as follows:

"12 Recital 4 in the preamble to Directive 2006/24 states:

'Article 15(1) of Directive 2002/58/EC sets out the conditions under which Member States may restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of that Directive. Any such restrictions must be necessary, appropriate and proportionate within a democratic society for specific public order purposes, i.e. to safeguard national security (i.e. State security), defence, public security or the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications systems.'

13 According to the first sentence of recital 5 in the preamble to Directive 2006/24, '[s]everal Member States have adopted legislation providing for the retention of data by service providers for the prevention, investigation, detection, and prosecution of criminal offences'.

14 Recitals 7 to 11 in the preamble to Directive 2006/24 read as follows:

'(7) The Conclusions of the Justice and Home Affairs Council of 19 December 2002 underline that, because of the significant growth in the possibilities afforded by electronic communications, data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention, investigation, detection and prosecution of criminal offences, in particular organised crime.

(8) The Declaration on Combating Terrorism adopted by the European Council on 25 March 2004 instructed the Council to examine measures for establishing rules on the retention of communications traffic data by service providers.

(9) Under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) [signed in Rome on 4 November 1950], everyone has the right to respect for his private life and his correspondence. Public authorities may interfere with the exercise of that right only in accordance with the law and where necessary in a democratic society, inter alia, in the interests of national security or public safety, for the prevention of disorder or crime, or for the protection of the rights and freedoms of others. Because retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organised crime and terrorism, it is necessary to ensure

that retained data are made available to law enforcement authorities for a certain period, subject to the conditions provided for in this Directive. …

(10) On 13 July 2005, the Council reaffirmed in its declaration condemning the terrorist attacks on London the need to adopt common measures on the retention of telecommunications data as soon as possible.

(11) Given the importance of traffic and location data for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure at European level that data that are generated or processed, in the course of the supply of communications services, by providers of publicly available electronic communications services or of a public communications network are retained for a certain period, subject to the conditions provided for in this Directive.'

15 Recitals 16, 21 and 22 in the preamble to Directive 2006/24 state:

'(16) The obligations incumbent on service providers concerning measures to ensure data quality, which derive from Article 6 of Directive 95/46/EC, and their obligations concerning measures to ensure confidentiality and security of processing of data, which derive from Articles 16 and 17 of that Directive, apply in full to data being retained within the meaning of this Directive.

(21) Since the objectives of this Directive, namely to harmonise the obligations on providers to retain certain data and to ensure that those data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of this Directive, be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.

(22) This Directive respects the fundamental rights and observes the principles recognised, in particular, by the Charter of Fundamental Rights of the European Union. In particular, this Directive, together with Directive 2002/58/EC, seeks to ensure full compliance with citizens' fundamental rights to respect for private life and communications and to the protection of their personal data, as enshrined in Articles 7 and 8 of the Charter.'

58. The main purpose of Directive 2006/24/EC was to harmonise Member States' provisions concerning the retention of certain data which are generated or processed by providers of publicly available electronic communications services or of public communications networks. It required the providers of publicly available electronic communications services or public communications networks to retain traffic and location data belonging to individuals or legal entities. Such data included the calling telephone number and name and address of the subscriber or register user, user IDs (a unique identifier assigned to each person who signs with an electronic communications service), Internet protocol addresses, the numbers dialled, and call forwarding or call transfer records. The retention period was to last for a minimum period of six months and up to two years, and the sole purpose of processing and storing the data was to prevent, investigate, detect, and prosecute serious crimes, such as organized crime and terrorism. It did not, however, permit the retention of the content of the communication or of information consulted.

59. There were two further EU instruments which were not alluded to, or opened, to the court below by counsel on either side, although they perhaps should have been, a matter in respect of which the trial judge, who discovered them through her own researches, was robustly critical. These were, namely Directive EU 2016/680 of the European Parliament and of the Council of 27 April 2016 (otherwise known as the Data Protection Law Enforcement Directive (or LED) 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; and Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 (otherwise known as the General Data Protection Regulation or GDPR) 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.

60. In fairness to counsel, although both instruments had been passed by the European Parliament and Council on the 27th of April 2016, on the EU statute book, so to speak, neither of them was in fact in force in Ireland at the date of the trial In the case of Regulation (EU) 2016/679 (i.e. the GDPR), which was intended to be directly effective, while that instrument had become law on the 24th of May 2016, 21 days after its publication in the Official Journal of the EU, but it was not to apply until the 25th of May 2018. In contrast, Directive EU 2016/680 was not intended to be directly effective and therefore possibly, and indeed almost certainly in the case of Ireland, it would require transposition. The date by which Ireland was required to ensure transposition was in fact the 6th of May 2018. This transposition was subsequently achieved through the Data Protection Act, 2018, primarily through 'Part 5 – Processing of Personal Data for Law Enforcement Purposes'.

61. The potential relevance of Directive EU 2016/680, and Regulation (EU) 2016/679, as the trial judge saw it, is that these instruments elaborated yet further on how the concept of "personal data" is to be understood in EU law. Both the Directive and the Regulation define personal data as: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

62. Moreover, recital 21 to Directive EU 2016/680 states:

"The principles of data protection should apply to any information concerning an identified or identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is no longer identifiable."

63. In the *Digital Rights and Landesregierung* cases the Irish High Court and the Constitutional Court of Austria (the Verfassungsgerichtshof) had each respectively, in the context of domestic litigation at hearing before them, submitted requests to the CJEU for preliminary rulings as to the validity of Directive 2006/24/EC, in particular in the light of two fundamental rights under the Charter, namely the fundamental right to respect for private life (Article 7) and the fundamental right to the protection of personal data (Article 8). As essentially the same query was being raised in both cases the CJEU dealt with them together.

64. The CJEU considered the controversial measure as a whole, both in its own terms, and having regard to the legislative scheme of which it was a part, and concluded that the data it required to be retained made it possible, in particular, (1) to know the identity of the person with whom a subscriber or registered user has communicated and by what means; (2) to identify the time of the communication as well as the place from which that communication took place and (3) to know the frequency of the communications of the subscriber or registered user with certain persons during a given period. Those data, taken as a whole, could provide very precise information on the private lives of the persons whose data were retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, activities carried out, social relationships and the social environments frequented. The Court took the view that, by requiring the retention of those data and by allowing the competent national authorities to access those data, the Directive interfered in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data.

65. Furthermore, the fact that data are retained and subsequently used without the subscriber or registered user being informed was likely to generate in the persons concerned a feeling that their private lives were the subject of constant surveillance. The Court then examined whether such an interference with the fundamental rights at issue was justified. It stated that the retention of data required by the Directive was not such as to adversely affect the essence of the fundamental rights to respect for private life and to the protection of personal data. The Directive did not permit the acquisition of knowledge of the content of the electronic communications as such and provided that service or network providers must respect certain principles of data protection and data security. Furthermore, the retention of data for their possible transmission to the competent national authorities genuinely satisfied an objective of general interest, namely the fight against serious crime and, ultimately, public security. However, the Court was nevertheless of the opinion that, by adopting Directive 2006/24/EC, the EU legislature had exceeded the limits imposed by compliance with the principle of proportionality. In that context, the Court observed that, in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by the Directive, the EU legislature's discretion was reduced, with the result that review of that discretion should be strict. Although the retention of data required by the Directive might be appropriate for attaining the objective pursued by it, the wide-ranging and particularly serious interference of the Directive with the fundamental rights at issue was not sufficiently circumscribed to ensure that that interference was actually limited to what was strictly necessary.

66. The CJEU specifically noted, firstly, that the Directive covered, in a generalised manner, all individuals, all means of electronic communication and all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.

67. Secondly, the Directive failed to lay down any objective criterion which would ensure that the competent national authorities could have access to the data and use them only for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights in question, may be considered to be sufficiently serious to justify such an interference. On the contrary, the Directive simply referred in a general manner to 'serious crime' as defined by each Member State in its national law. In addition, the Directive did not lay down substantive and procedural conditions under which the competent national authorities might have access to the data and subsequently use them. In particular, access to such data was not made dependent on prior review by a court or by an independent administrative body.

68. Thirdly, so far as concerned the data retention period, the Directive imposed a period of at least six months, without making any distinction between categories of data based on the persons concerned or the possible usefulness of the data in relation to the objective being pursued. Furthermore, that period was set at between a minimum of six months and a maximum of 24 months, but the Directive did specify objective criteria on the basis of which the period of retention should be determined in order to ensure that it was limited to what was strictly necessary.

69. The Court also found that the Directive did not provide for enough safeguards to ensure effective protection of the data against the risk of abuse and against any unlawful access and use of the data. It also noted, *inter alia*, that the Directive permitted service providers to have regard to economic considerations when determining the level of security which they would apply and that it did not ensure the irreversible destruction of the data at the end of their retention period.

70. Fourthly, the CJEU stated that the Directive did not require that the data be retained within the EU. Therefore, the Directive did not fully ensure the control of compliance with the requirements of protection and security by an independent authority, as was, however, explicitly required by the Charter. Such a control, carried out on the basis of EU law was, in the CJEU's view, an essential component of the protection of individuals with regard to the processing of personal data.

71. Having regard to all of these circumstances the CJEU declared Directive 2006/24/EC to be invalid.

72. Following the CJEU's decision in the *Digital Rights and Landesregierung* cases there was uncertainty as to exactly how far reaching its implications were, particularly in circumstances where Directive 2006/24/EC had been enacted to amend Directive 2002/58/EC. The question was, to what extent did the ruling in the *Digital Rights and Landesregierung* cases impact the earlier directive the validity of which had not been challenged in those cases. This uncertainty gave rise to two further cases in which preliminary rulings were sought from the CJEU in the hope of obtaining greater clarity, and for convenience these were also conjoined and heard together. These were cases no's C-203/15 *Tele2 Sverige AB v Post och telestyrelsen*, and C-698/15 *Secretary of State for the Home Department v Watson and others* ("*the Tele2 Sverige and Watson cases*").

73. The background to the *Tele2 Sverige* case was that on the 9th April 2014, Tele2 Sverige, a provider of electronic communications services established in Sweden, informed the Post och telestyrelsen ("PTS"), being the Swedish Post and Telecom Authority, that, following the ruling in the *Digital Rights* and *Landesregierung* cases that Directive 2006/24/EC was invalid, it would cease, as from 14 April 2014, to retain electronic communications data, covered by the relevant Swedish national law providing for such retention in purported transposition of, inter alia, Directive 2006/24/EC , and that it would erase data retained prior to that date. On 15 April 2014, the Rikspolisstyrelsen (the Swedish National Police Authority) sent to the PTS a complaint to the effect that Tele2 Sverige had ceased to send to it the data concerned. In parallel with this development, the Swedish Minister for Justice appointed a special rapporteur to examine the relevant Swedish legislation in the light of the judgment in the *Digital Rights and Landesregierung* cases. The special rapporteur was of the opinion that the *Digital Rights* judgment could not be interpreted as meaning that the general and indiscriminate retention of data was to be condemned as a matter of principle. From his perspective, neither should the *Digital Rights*

judgment be understood as meaning that the Court had established, in that judgment, a set of criteria all of which had to be satisfied if legislation was to be able to be regarded as proportionate. He considered that it was necessary to assess all the circumstances to determine the compatibility of the Swedish legislation with EU law, such as the extent of data retention in the light of the provisions on access to data, on the duration of retention, and on the protection and the security of data.

74. Relying on this opinion the PTS ordered Tele2 Sverige to commence retention of data no later than the 25th of July 2014. Tele2 Sverige challenged the legality of this order before the Stockholm Administrative Court, arguing that the special rapporteur's opinion had been based on a misinterpretation of the *Digital Rights* ruling, and in the course of this litigation the Stockholm Administrative Court sought a preliminary ruling from the CJEU, asking, *inter alia*: is a general obligation to retain traffic data covering all persons, all means of electronic communication and all traffic data without any distinctions, limitations or exceptions for the purpose of combating crime … compatible with Article 15(1) of Directive 2002/58/EC, taking account of Articles 7 and 8 and Article 52(1) of the Charter?

75. A largely similar question was referred by a Divisional Court, sitting in the Queen's Bench Division of the High Court of England and Wales in the *Watson* case. The context there was a challenge by way of judicial review to the legality of s.1 of the UK's Data Retention and Investigatory Powers Act 2014 (DRIPA).

76. Commenting on the effect of Directive 2002/58/EC the CJEU stated in its judgment in the *Tele2 Sverige and Watson* cases that:

> "Like Directive 95/46/EC … this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms."

77. The CJEU observed that a determination of the scope of Directive 2002/58/EC must take into consideration, *inter alia*, the general structure of that directive. It considered that, having regard to the general structure of Directive 2002/58/EC, factors such as such as safeguarding national security, defence and public security and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications system, do not permit the conclusion that the legislative measures referred to in Article 15(1) of Directive 2002/58/EC are excluded from the scope of that directive, for otherwise that provision would be deprived of any purpose. Indeed, Article 15(1) necessarily presupposes that the national measures referred to therein, such as those relating to the retention of data for combating crime, fall within the scope of that directive, since it expressly authorises the Member States to adopt them only if the conditions laid down in the directive are met.

78. The CJEU considered that the scope of Directive 2002/58/EC extended to a legislative measure, such as that at issue in the main proceedings, that required providers of electronic communications services to retain traffic and location data, since to do so necessarily involved the processing, by those providers, of personal data. The CJEU further held that the scope of that directive also extended to a legislative measure relating to the access of the national authorities to the data retained by the providers of electronic communications services.

79. As stated in its recital 2, Directive 2002/58/EC seeks to ensure full respect for the rights set out in Articles 7 and 8 of the Charter. To that end Article 5(1) of that directive provides that the Member States must ensure, by means of their national legislation, the confidentiality of communications effected by means of a public communications network and publicly available electronic communications services, and the confidentiality of the related traffic data. This principle of confidentiality of communications implies, inter alia, as stated in the second sentence of Article 5(1) of that directive, that, as a rule, any person other than the users is prohibited from storing, without the consent of the users concerned, the traffic data related to electronic communications. The only exceptions relate to persons lawfully authorised in accordance with Article 15(1) of that directive and to the technical storage necessary for conveyance of a communication.

80. The CJEU went on to state that in so far as Article 15(1) of Directive 2002/58/EC enables Member States to restrict the scope of the obligation of principle to ensure the confidentiality of communications and related traffic data, that provision must, in accordance with the Court's settled case-law, be interpreted strictly. In the CJEU's opinion that provision cannot, therefore, permit the exception to that obligation of principle and to the prohibition on storage of data, laid down in Article 5 of Directive 2002/58/EC, to become the rule, if the latter provision is not to be rendered largely meaningless.

81. The CJEU observed that the first sentence of Article 15(1) of Directive 2002/58 provides that the objectives pursued by the legislative measures that it covers, which derogate from the principle of confidentiality of communications and related traffic data, must be 'to safeguard national security — that is, State security — defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system', or one of the other objectives specified in Article 13(1) of Directive 95/46, to which the first sentence of Article 15(1) of Directive 2002/58 refers. That list of objectives is exhaustive, as is apparent from the second sentence of Article 15(1) of Directive 2002/58, which states that the legislative measures must be justified on 'the grounds laid down' in the first sentence of Article 15(1) of that directive. Accordingly, the Member States cannot adopt such measures for purposes other than those listed in that latter provision. Further, the CJEU considered that Article 15(1) of Directive 2002/58/EC must be interpreted in the light of the fundamental rights guaranteed by the Charter.

82. Accordingly, in the CJEU's view, the importance both of the right to privacy guaranteed in Article 7 of the Charter, and of the right to protection of personal data guaranteed in Article 8 of the Charter, as derived from the Court's case-law must be taken into consideration in interpreting Article 15(1) of Directive 2002/58. The same is true of the right to freedom of expression, guaranteed in Article 11 of the Charter, in the light of the importance accorded to that freedom in any democratic society.

83. Under Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and must respect the essence of those rights and freedoms. With due regard to the principle of proportionality, limitations may be imposed on the exercise of those rights and freedoms only if they are necessary and if they genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.

84. At paragraph 95 of the CJEU's judgment, it was remarked that with respect to that last issue, the first sentence of Article 15(1) of Directive 2002/58 provides that Member States may adopt a measure that derogates from the principle of confidentiality of communications and related traffic data where it is a 'necessary, appropriate and proportionate measure within a democratic society', in view of the objectives laid down in that provision. As regards recital 11 of that directive, it states that a measure of that kind must be 'strictly' proportionate to the intended purpose. In relation to the retention of data, the requirement laid down in the second sentence of Article 15(1) of that directive is that data should be retained 'for a limited period' and be 'justified' by reference to one of the objectives stated in the first sentence of Article 15(1) of that directive.

85. In considering whether the national legislation at issue in the Tele 2 Sverige case satisfied those conditions, the CJEU noted that that legislation provided for a general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication, and that it imposed on providers of electronic communications services an obligation to retain that data systematically and continuously, with no exceptions. In that regard, the categories of data covered by that legislation corresponded, in essence, to the data whose retention was required by Directive 2006/24/EC.

86. The CJEU observed that the data which providers of electronic communications services in Sweden were required to retain under the legislation at issue made it possible to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to establish the location of mobile communication equipment. That data included, *inter alia*, the name and address of the subscriber or registered user, the telephone number of the caller, the number called and an IP address for internet services. That data made it possible to identify the person with whom a subscriber or registered user had communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. Further, that data made it possible to know how often the subscriber or registered user communicated with certain persons in a given period.

87. In the CJEU's opinion, such data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them. That data provides the means of establishing a profile of the individuals concerned, information that is no less sensitive, in the CJEU's view, having regard to the right to privacy, than the actual content of communications.

88. The CJEU considered that the interference entailed by such legislation in the fundamental rights enshrined in Articles 7 and 8 of the Charter is very far-reaching and must be regarded as particularly serious. The fact that the data is retained without the subscriber or registered user being informed is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance. Moreover, even if such legislation does not permit retention of the content of a communication and is not, therefore, such as to affect adversely the essence of those rights, the retention of traffic and location data could nonetheless have an effect on the use of means of electronic communication and, consequently, on the exercise by the users thereof of their freedom of expression, guaranteed in Article 11 of the Charter.

89. The CJEU felt that given the seriousness of the interference in the fundamental rights concerned represented by national legislation which, for fighting crime, provides for the retention of traffic and location data, only the objective of fighting serious crime is capable of justifying such a measure. Further, while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight.

90. In the CJEU's view, under the Swedish national legislation at issue the retention of traffic and location data is the rule, whereas the system put in place by Directive 2002/58 requires the retention of data to be the exception. Further, it was objectionable on the basis that it covered, in a generalised manner, all subscribers and registered users and all means of electronic communication as well as all traffic data, and provided for no differentiation, limitation or exception according to the objective pursued. The legislation in controversy did not require there to be any relationship between the data which must be retained and a threat to public security. In particular, it was not restricted to retention in relation to (i) data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to fighting crime.

91. In the CJEU's view the legislation in question exceeded the limits of what was strictly necessary and could not be justified, within a democratic society, as required by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter.

Implications for the Act of 2011

92. Having listened to the arguments on both sides, we are in no doubt that the appellant's contention that the legality of Act of 2011 is now questionable has both strength and cogency, particularly having regard to the litigation described (both the *Digital Rights* and *Landesregierung* cases, and the *Tele2 Sverige and Watson cases*) and the jurisprudence resulting therefrom. In addition, we have taken account of the High Court's recent decision in *Dwyer v The Commissioner of An Garda Siochána, Ireland & Ors* [2018] IEHC 685. The Dwyer decision declared ss 3(1) and 6(1) of the Act of 2011 to be incompatible with EU law, in effect as being inconsistent with and failing to adequately respect Articles 7 and 8 of the Charter. The High Court Judge was considering the possibility of also making a declaration of incompatibility with the ECHR under s. 5 of the European Convention on Human Rights Act, 2003 but it is unclear from the judgment whether or not he was ultimately willing to do so. We note that the *Dwyer* case was concerned with mobile telephony data, and not e-mail and internet data, and that separate parts of Second Schedule of the Act of 2011 apply to each of these. We further understand that the judgment in the *Dwyer* case may be under appeal. Nevertheless, it provides some additional support for the approach that we are prepared to adopt. While it is not open to this court to either condemn or uphold the legislation in question in the context of the present proceedings, we cannot ignore the developments that have taken place, particularly having regard to the supremacy of EU law in this area. Accordingly, for the purposes of the admissibility argument, we are prepared, without deciding the issue definitively, to assume (a) that it was reasonable to ask that the Act of 2011 should be disapplied, and (b) the absence of a lawful power on the part of Eircom / Eircom Indigo to retain the data at issue in these proceedings, namely that which was furnished by them to An Garda Siochána pursuant to the requests made of them in that regard by Chief Superintendents Kirwan and Gilligan, respectively. Further, and again without deciding the issue definitively, we are prepared to assume the absence of a lawful power on the part of the said Chief Superintendents to access that data.

Implications for the admissibility issue

93. It is important not to lose sight of the fact that the objection in this case was to the admissibility of the evidence in question on

the basis that it was, in effect, both illegally obtained and obtained in breach of certain of the appellant's constitutional and Charter rights.

94. Before considering the specific contentions of the appellant and the respondent, it should be observed that there has never been an absolute, or near absolute, exclusionary rule in respect of evidence obtained in circumstances which does not violate an accused person's constitutional rights. In the case of illegally obtained evidence, without an associated violation of the accused's constitutional rights, it has long been the law that a trial judge may admit (or exclude) such evidence as a matter of discretion. See *People (Attorney General) v O'Brien* [1965] I.R. 142. In such circumstances factors which might influence how the discretion would be exercised would include the circumstances in which the illegality occurred, whether the illegality was adverted to or not, the existence of a bona fide mistaken belief as to legality, the extent of the prejudice caused (if any), and considerations of fairness and justice; to name but some.

95. For very many years, the situation was much more restricted in the case of evidence obtained in deliberate and conscious violation of the accused person's constitutional rights, in the absence of extraordinary excusing circumstances. Following the decision in the *People (Director of Public Prosecutions) v Kenny* [1990] 2 I.R. 110, there was a near absolute exclusionary rule where there had been such a violation. In relatively recent times, however, the Supreme Court, by a 4:3 majority, in the case of *J.C. v DPP (No 1)* [2015] IESC 31, somewhat relaxed the near absolute exclusionary rule, and outlined a new approach that would strike what was considered to be a more appropriate balance between the competing needs to hold the Gardaí to account on the one hand, and society's interest, including that of the victim's of crime, in ensuring that those who breach the criminal law are convicted and punished. The absolute or near absolute exclusionary rule was considered to operate too harshly in some cases, particularly where the breach of rights had been inadvertent and unintended.

96. Following *JC*, the position is now, as set out in paragraph 5.5 of the judgment of Clarke J (as he then was) in that case, that:

> *"Where objection is taken to the admissibility of evidence on the grounds that it was taken in circumstances of unconstitutionality, the onus remains on the prosecution to establish either: -*
>
> > *(a) that the evidence was not gathered in circumstances of unconstitutionality; or*
> >
> > *(b) that, if it was, it remains appropriate for the court to nonetheless admit the evidence.*
>
> *The onus in seeking to justify the admission of evidence taken in unconstitutional circumstances places on the prosecution an obligation to assert the basis on which it is said that the evidence should, nonetheless, be admitted AND ALSO to establish any facts necessary to justify such a basis."*

97. Although the issue was not specifically argued before us, we would add as *an obiter dictum*, that we know of nothing in the law of Ireland to suggest that, where a court is concerned with the admissibility of evidence obtained in breach of a fundamental personal right guaranteed to an accused under an international instrument such as the Charter, or the ECHR, but which is not directly mirrored in the Constitution of Ireland, such breaches are to be approached in the same way as breaches of rights guaranteed to the accused under the Irish Constitution, or that they engage the same exclusionary rules.

The appellant's case on admissibility of the retained data.

98. The appellant's case, as it is understood by this court, is multi-layered. First, she is saying simply that the evidence was obtained illegally, i.e., retained by Eircom /Eircom Indigo without lawful authority and that, it having been so retained, unlawful access to it was granted by those parties to An Garda Siochána, and that the trial judge ought to have exercised her discretion to exclude it. We have indicated that, for the purposes of the argument but without deciding the issue, we are prepared to assume the correctness of that contention that the evidence was obtained without lawful authority. The appellant makes the case that the evidence which she says was illegally obtained was obtained in breach of EU law and reliance is placed on the primacy of EU law. In essence, her case is that in circumstances where EU legislative policy on data retention is explicit, and so strong in its terms, neither the trial court, nor this Court, is at liberty to disregard it, and that in effect the discretion could only be exercised in one way, namely to exclude the evidence.

99. Secondly, she is making the case that both constitutional and Charter rights to the benefit of which she was entitled were breached. In that regard, on the *voir dire* on this admissibility issue in the court below, counsel for the appellant variously submitted:

> *"Now, the issue that arises, Judge, is fundamentally the right of privacy. And it's the right of privacy as defined in our own constitution but with more than a passing reference to how privacy has been defined within the European Union and within European case law."*

(transcript, D5, P25,L1-4)

> *"…it seems to me that this is a breach of a significant European right, a breach of privacy"*

and:

> *"It's a right, in my respectful submission, which is a constitutional right. It is a right under the Charter and it is under Irish jurisprudence one of the highest breaches of rights that could have occurred and, in my respectful submission, there's no inadvertence here."*

(transcript, D6, P35,L15-16 and 23-26)

100. She has invoked the unenumerated right to privacy that arises in certain circumstances under Article 40.3 of the Irish Constitution. Accordingly, it is contended, the more restrictive exclusionary rule (as originally formulated in the *Kenny* case, and as recently modified in the *J.C.(No1*) case, that is potentially engaged where a breach of a constitutional right is alleged, is in fact engaged here. However, nowhere in the appellant's written submissions, nor in the oral submissions to this court in amplification of the written submissions, does the appellant particularise exactly how her said constitutional right is said to have been allegedly breached.

101. In addition, the appellant has explicitly suggested through her counsel in the court below, that she personally has suffered a breach of her right to privacy guaranteed under Article 7 of the Charter. While there is no doubt but that that case was made, there

was no express mention of reliance by her on any alleged breach of the right to the protection of personal data, or of the right to freedom of expression, respectively guaranteed under Articles 8 and Article 11 of the Charter, nor of any cognate or analogous rights guaranteed under the ECHR. Again, it bears remarking upon, that apart from baldly asserting a breach of the right to privacy, nowhere in the appellant's written submissions, nor in the oral submissions to this court, does the appellant engage with the actual facts of the case in order to particularise exactly how her right to privacy under Article 7 of the Charter is said to have been allegedly breached.

102. Moreover, bearing in mind our *obiter* remarks at paragraph 94 above, even if there was a breach of the appellant's Article 7 Charter rights, it would not, unless the Article 7 right was exactly mirrored in the Irish Constitution, engage the more restrictive exclusionary rule on that account alone. Rather, any such breach would simply be one of several factors to be weighed by the court seized of the admissibility issue in determining whether to exercise its discretion in favour of admitting the evidence.

The respondent's submissions on this admissibility issue

103. Counsel for the respondent has argued forcibly that the subscriber and traffic data retained by Eircom /Eircom Indigo was not personal data relating to the appellant. As we have seen "personal data" means any information relating to an identified or identifiable natural person described as the "data subject". Such data as those telecommunications service providers had, when combined with the IP addresses supplied to them by An Garda Siochána, who in turn had obtained those addresses from a source outside of the European Union, namely indirectly from Hush Communications Canada Incorporated by the lawful mechanism of a mutual assistance request, certainly allowed the internet café from which the traffic had originated to be identified, but it did not identify the appellant.

104. Moreover, the respondent argues, it also did not render the appellant identifiable. The respondent argues that the only information to which the applicable EU laws can apply is electronically stored communications information from which a person can be identified either directly or indirectly. It was not possible from the combined electronically stored communications information processed, or available for processing, in this case, to identify the appellant either directly or indirectly. Other evidence, not involving electronically stored communications data, was required to effect the identification, namely that provided by the investigating Gardaí who identified a person of interest in the course of their investigations, and who showed a photo of that person to Mr Babu Kandru, and the evidence of Mr Babu Kandra and of the Gardai involved in the events that transpired at the internet café on the 28th of September 2013.

105. In summary, the respondent's case is that even if there was no lawful authority for the subscriber data in question to be retained, or for that which was retained to be accessed, there is no question of the appellant's constitutional right to privacy, or any other rights of the appellant, whether that be her right to privacy under Article 7 of the Charter, or any other of her rights, having been breached.

106. Moreover, it was argued, even if there was a breach of the appellant's constitutional right to privacy it had occurred in circumstances where reliance had been placed on the Act of 2011, which was in force at the time and had not been expressly condemned by any court, and accordingly the breach was inadvertent and ought to be forgiven in the circumstances. In that regard it was relevant that the request to Eircom under s.6(1) of the Act of 2011 was made on the 20th of March 2013, and the request to Eircom Indigo was made on the 17th of August 2012, both requests predating the CJEU's judgment in the *Digital Rights* and *Landesregierung* cases which was delivered on the 8th of April 2014.

107. Before considering the trial judge's ruling on this issue, it may be convenient to briefly describe the second admissibility issue raised, which was in relation to evidence concerning the information obtained in Canada, as the trial judge dealt with both issues in the same ruling.

The information obtained in Canada

108. Regarding the information obtained from Canada, and specifically that ultimately given by Steven Olaf Youngman and Darryl Krassman in respect of the data obtained from Canada, the court of trial was also asked to rule this inadmissible, and it is contended that the trial judge was wrong to exercise her discretion in favour of admitting it.

109. The data at issue comprised the IP addresses from which the emails in controversy had originated, and the identity of the Irish telecommunications providers, namely Eircom and Eircom Indigo, through whose network the communications had been routed via an account or accounts of one or more of their (i.e., Eircom's and Eircom Indigo's) subscribers, the identity of which was/were at that point unknown. As has already been stated, the Canadian data when combined with subscriber and traffic data retained by Eircom and Eircom Indigo rendered it possible to identify the subscriber account or accounts in question, namely accounts in the name of an entity called Y & T Infotech, which operated an internet café trading as "Wired" at 15 Aungier St, Dublin 2, and which was owned by the aforementioned Mr Babu Kandra.

110. In support of the application that the data obtained from Canada, and evidence concerning it, should be ruled inadmissible, counsel for the appellant submitted, both to the court below, and again to us, that the court of trial had no evidence concerning how and where the data which was ultimately provided had been held or stored,, concerning who else might have had access to it, and whether any safeguards were in place to protect the data subject's rights. It was further complained that the procedural history concerning how the mutual assistance request was processed by the Canadian authorities was vague, and that the evidence gathering order of Chief Justice Cullen of the Supreme Court of British Columbia had neither been exhibited nor otherwise proven. Moreover, there was no evidence before the court concerning the data protection laws (if any) in Canada, and whether they had been respected, or concerning whether such laws, if they exist, provide the same level of protection for personal data as is provided in the EU and to the benefit of which the appellant was said to be entitled.

111. In reply to this, counsel for the respondent has argued, both in this court and in the court below, that EU data protection rules have no application to how electronic communications data in the possession of a party in a non-EU country may be retained, processed or accessed by another party within that country. It was submitted that what matters is that the data was obtained on foot of a lawful court order issued in Canada, and that it was passed on to the Irish authorities through the well-recognised and lawful procedure of a formal inter state request for mutual legal assistance. The court below had sworn testimony that this was how the data in question was obtained, and that the evidence gathering order at issue had been applied for to, and that it was granted by, the Supreme Court of British Columbia. There was no evidence to the contrary or to suggest any legal deficiency in the process. A witness from Hush Communications Canada Incorporated had confirmed on oath that his company had been served with the evidence gathering order, and that they had provided the data at issue to the Canadian police on foot of it. It was not necessary in the circumstances to exhibit the Canadian court order.

The trial judge's ruling on the admissibility issue

112. The trial judge ruled as follows:

> *"JUDGE: Thank you. Now, this application concerns an application on behalf of the accused seeking the exclusion of evidence contained in two print documents, MF1 and MF2, obtained by the prosecution on foot of data retention requests made to Eircom pursuant to section 6(1) of the 2011 Communications (Retention of Data) Act and also a number of CDs which were provided by Hush.com to the Irish authorities on foot of a court order made by a court in Vancouver in Canada in 2015.*
>
> *It is submitted on behalf of the accused that the manner in which the data was stored and accessed here in Ireland and the means by which the records were accessed in Canada both contravene the accused's fundamental right to privacy, a right which is afforded protection by the European directives, which have been opened to me, by the Charter of Fundamental Rights of the European Union and by the Irish Constitution. It is submitted that the breadth of the 2011 Act and its absence of safeguards put it in flagrant breach of EU law, as stated in the Digital Rights decision of 2014 and the Tele2 Sveriga decision of 2016. Mr O'Higgins submits that if I accept that the 2011 Act is in breach of EU law, as EU law has primacy over national law, I am mandated to disapply the 2011 Act and I must rule the evidence inadmissible.*
>
> *The documents received from Eircom, namely MF1 and MF2, provide details concerning the IP address, date, time, landline number and geographical location from which emails relevant to the investigation were sent. The ability of investigating members to furnish Eircom with the subscriber details was dependent on their gaining access to the IP address at which the accounts were created and from which emails were sent. The emails in question were all sent from Hushmail accounts. Hush.com is a Canadian web-based company which offers an encrypted email service.*
>
> *The IP addresses from which the email accounts were created and used were available to Mr Finnerty on the 20th of August 2012 and the 14th of March 2013. The evidence in the voir dire did not establish how this information came to Mr Finnerty, but as it was not compelled by a court order, its disclosure appears to be informal and voluntary. In 2015, as a consequence of an order made against Hush.com, a full snapshot of the named accounts was created by Mr Krassman from Hush, which provided the IP, the activity logs and the content of email folders. This was disclosed to the Irish authorities by the Canadian authorities.*
>
> *The evidence of Mr Steve Youngman established that because all of the accounts in question were set up without payment, Hush.com did not have any registration, billing or payment information for any of the named accountholders, nor did they have any correspondence to, from or on behalf of the subscribers. As the accused was not a named accountholder, the email accounts were either not of her creation or they were created by her under a pseudonym.*
>
> *The arguments advanced in support of the application to exclude are predicated on the assumption that the material contained in MF1 and MF2 amounts to personal data and that the content of the emails contained within the folders is such that there is an expectation that a right of privacy would attach to that content. The rights in question, Mr O'Higgins maintains, is afforded protection by the data retention legislation, both at national and European level.*
>
> *Mr Naidoo's argument in reply is that all of Mr O'Higgins's arguments fall at the first hurdle, because neither the IP address of the email accounts, however obtained, nor the data contained in MF1 or MF2, amount to personal data and the content of the emails which were sent from the various accounts do not attach a right of privacy, as they were intended for circulation among a number of individuals to whom they were addressed, and furthermore, the content of those emails contains data which is personal to the subject of those emails, but in no way identifies any material which affects the privacy rights of the accused.*
>
> *Now, the Court has been operating on an assumption that the legislation submitted and cited comprehensively represents the current EU position on the protection of personal data. However, it does that appear that two significant and substantive enactments of EU law have come into force since May of 2016 and they are regulation 679 of 2016 and directive 680 of 2016. The enactments do not materially alter the definition of personal data. However, they do expand on the definition contained in EC directive 46 of 95 and they provide elaborations which are relevant to this particular issue. Both the regulation and directive define personal data as: "'Personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name identification, an identification number, location data, an online identifier or to one of more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person."*
>
> *Recital 21 of the regulation number 680 of 2016 states: "The principles of data protection should apply to any information concerning an identified or identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all the objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should not therefore apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or personal data rendered anonymous."*
>
> *For the purpose of my ruling, I have also consulted opinion numbered 4 of 2007 of the Article 29 Data Protection Working Party, which addressed the concept of personal data and whose objective was to come to a common understanding of the concept of personal data. The opinion breaks down and analyses each of the four elements of the definition of personal data, namely any information being the first; the second being the concept of relating to; the third being identified or identifiable; and the last being a natural person. It deals with what could or could not come within the scope of each of those four elements.*
>
> *In his submission, Mr Naidoo has invited the Court to look at what digital data was in fact recovered in this case and he has analysed the content of MF1 and MF2, in addition to the content of the emails obtained from the Canadian disclosure, and he is arguing that no element of the data could lead to the identification of the accused either directly or indirectly. Mr Naidoo indicates that the evidence which links the accused to the sending of the emails comes from direct witness testimony. The material received from Canada was encrypted and could not be accessed without being de-*

encrypted by the service provider. It is also noteworthy that Hushmail did not hold or provide any information from which the accused could be identified other than an IP address linked to an internet café. Insofar as the Canadian service provider was concerned, the anonymity of the purported accountholders was maintained throughout.

Mr Naidoo then referred the Court to the 2016 decision of Patrick Breyer v. Bundesrepublik Deutschland, which he maintains is authority for the proposition that in order to amount to data, the identifying element of the data must come from the digital data itself, which data may emanate from one digital source or multiple digital sources. He maintains that if what was contained in the items at issue in this particular application contained anyone's personal data, it was that of the internet café owner and that of [the complainant], and if anyone's privacy rights have been infringed, it is their rights, but not those of the accused.

Mr O'Higgins in reply maintains that the data contained in the Irish and Canadian material is personal data in the sense of being location data from which it is possible to identify the accused. I have considered whether the content of emails to various addressees constitutes personal data of the accused and whether it is private. It is not unreasonable to infer that the intention of the writer of these emails did not have any intention to keep the information contained in them private. In addition, the content of the email, insofar as it contains personal data, contains personal data in respect of [the complainant], of which she would have a reasonable expectation of privacy.

I have next considered whether there is any element of the Canadian information or the data in MF1 and MF2 which could lead to the identification of the accused by reference to her location or otherwise and I am quite satisfied that there is no element of the data which provides that vital identifying link to the accused. The link must therefore be established by evidence other than digital evidence. I have then considered whether, in the absence of any identifiable link to the accused, it can be regarded as her location data. Location data should not be conflated with evidence as to location. Location data requires the presence of some means, either direct or indirect, by which the data subject can be identified. The material in this case, in my opinion, falls into the category of potential evidence as to location. I therefore find myself in agreement with Mr Naidoo's submission that there has been a failure on the part of the accused to establish that her rights to privacy have been infringed and the absence of such an interference is a complete answer to all of the applications and submissions made on behalf of the accused. This is so, in view of the fact that no issue has been taken in relation to non-compliance with the provisions of the 2011 Act itself, and therefore I am ruling that the material is admissible evidence."

113. The trial judge's ruling is criticised by the appellant on the basis that she erred in principle in ruling that the data was not personal data and that the privacy rights of the appellant were not engaged. It was submitted that, having regard to the types of data that were considered to constitute personal data in the judgment in the *Tele2 Sverige and Watson* cases, the data the subject matter of the applications under s.6(1) of the Act of 2011, and now at issue, does constitute personal data and is sufficient to identify the appellant, a prerequisite of the prosecution's use of this information at trial.

114. Counsel for the appellant was also critical of the trial judges references to Directive EU 2016/680 (the Data Protection Law Enforcement Directive or LED) and Regulation EU 2016/679 (the GDPR), in circumstances where defence counsel had not been on notice that regard would be had to them, and where he had not had an opportunity to make submissions with respect to their relevance, if any. In the circumstances counsel for the appellant applied for a discharge of the jury and this was refused. Ground of appeal no (iii) complains that the decision not to discharge the jury was erroneous.

Discussion and Decision on Grounds (i), (ii) and (iii) – Retention of Data

115. The trial judge's decision to admit the evidence in controversy was fundamentally correct in our judgment. It might, however, have been preferable if she had focussed more particularly on the precise legal nature of the challenges being mounted in terms of how they ought properly to be characterised under Irish law. These were all fundamentally admissibility challenges, but there are different types of admissibility challenges, and they required analysis in that respect.

116. The first issue, to which there are two components, relates to whether there was prima facie evidence of illegality and/or a breach of rights in how the evidence at issue was obtained.

117. It is appropriate to deal first with illegality. We have indicated a willingness to assume that it would have been appropriate for the trial judge to disapply the Act of 2011 as she was requested to do. In substance, the trial judge took exactly the same approach. The consequence of that is, that for purposes of this admissibility issue, Eircom/Eircom Indigo must be regarded as having had no lawful entitlement to retain the traffic and subscriber data at issue, nor to provide it to An Garda Siochána. Therefore, at a minimum, *People (Attorney General) v O'Brien* considerations were engaged, and the trial judge was obliged to consider whether in the exercise of her discretion she should admit, or exclude, the evidence in controversy.

118. The second component to the first issue relates to whether there was a breach of the appellant's rights in some respect. It is clear from the trial judge's ruling that she was fully alive to the fact that the appellant was arguing that her right to privacy in respect of her personal data, which she claimed was guaranteed both under the Constitution and under the Charter, was breached.

119. However, as we have seen, not all breaches of rights, assuming the existence of such a breach or breaches, will give rise necessarily to the same potential consequences in terms of a challenge to the admissibility of evidence obtained through such a breach or breaches. Breaches of non-constitutionally guaranteed rights, unless mirrored very closely in the Irish Constitution, would normally engage only the basic exclusionary rule expounded in *People (Attorney General) v O'Brien*, whereas breaches of constitutionally guaranteed rights would potentially engage the more restrictive exclusionary rule as recently modified in the *J.C. (No 1)* case.

120. It is clear that the accused was claiming both a breach of her unenumerated right to privacy, in so as it related to her personal data, arising under Article 40.3 of the Irish Constitution, as well as a breach of her right to privacy under Article 7 of the Charter. In that regard, the appellant's case was, and is, that the right to privacy guaranteed under Article 7, in so far as it relates to personal data, is at least as extensive, if not more extensive, than the unenumerated right to privacy guaranteed under the Irish Constitution. If she is correct about that, a breach of her Article 7 rights would arguably also engage the more restricted exclusionary rule that applies in the case of a breach of a right guaranteed by the Irish Constitution.

121. While is unquestionably the case that the appellant was asserting, and continues to assert, that her rights to privacy in respect of her personal data, guaranteed both under the Constitution and under the Charter, had been breached, the critical question is: is

she correct about this? If she is correct about this, then the court of trial was obliged to apply the more restrictive exclusionary rule, albeit in its recently modified form post the case of *J.C. (No 1)*, certainly to the extent that there was a breach of her rights under the Irish Constitution and, possibly, in respect of any concurrent breach of her rights under Article 7 of the Charter.

122. We have already commented that apart from baldly asserting a breach of her right to privacy, nowhere in the appellant's written submissions, nor in the oral submissions to this court, does the appellant engage with the actual facts of the case in order to particularise exactly how her constitutional right to privacy, (or for that matter her right to privacy under Article 7 of the Charter) is said to have been allegedly breached. We are prepared to infer that her case must be that data personal to her was retained by Eircom / Eircom Indigo and processed by them, including by the provision of access thereto to An Garda Siochána. However, the evidence, such as it is, does not bear out that what was retained and processed was data personal to her as the data subject. The data in question was not data personal to her, either in any quotidian sense, or in the sense in which it was understood in EU law as it applied on the day, namely as defined in Directive 95/46/EC, being "any information relating to an identified or identifiable natural person ('data subject')" where "an 'identifiable person' is one who can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

123. While the trial judge had some regard to the amplification of this definition in Directive EU 2016/680 and in Regulation EU 2016/679, which were not yet in force, the fact that she did so did not operate to the prejudice of the appellant. The amplified definition is, if anything, arguably more expansive in its embrace that the definition in Directive 95/46/EC and that would have been to the advantage of the appellant rather than to her disadvantage. We are satisfied that there is nothing in this point and that there was basis for discharging the jury as was requested by counsel for the appellant following the trial judge's ruling.

124. As the trial judge's ruling in effect makes clear, there was no electronically stored communications data in the possession of Eircom / Eircom Indigo, and furnished to An Garda Siochána, which either on its own, or indirectly by being combined with other electronically stored communications data, such as the IP addresses provided by Hush Communications Canada Incorporated, could have identified the appellant. At most such data could have identified the subscriber concerned as being the owner of the internet café, Mr Babu Kandra, but the appellant cannot rely on a possible breach of somebody else's right to the privacy of their personal data to support a claim that the more restrictive exclusionary rule is engaged and that it should result in the exclusion of the evidence concerned. In the circumstances we are not satisfied that there was enough evidence before the trial judge to establish that there had been any breach of a right to privacy in respect of the appellant's personal data, whether under the Constitution or, for that matter, under Article 7 of the Charter, sufficient to engage the more restrictive exclusionary rule. We consider therefore that the trial judge's findings that the data in question was not personal data, and that the appellant's privacy rights were not breached, were entirely correct.

125. It follows from the finding of insufficient evidence of a breach of rights that even if the appellant is correct in suggesting that the right to privacy in respect of one's personal data guaranteed under Article 7 of the Charter is at least as extensive as her constitutional right to such privacy, there was still a failure to demonstrate how the more restricted exclusionary rule could have been engaged in the absence of evidence that the right was breached and that the evidence in controversy was obtained in consequence of that breach.

126. In so far as the basic, discretionary, exclusionary rule, as expounded in the *People (Attorney General) v O'Brien*, and which is engaged in cases where evidence has been obtained illegally, is concerned; there was a clear basis in this case for exercising the discretion in favour of admitting the evidence and we consider that the trial judge did not err, and was indeed correct, in doing so. The data at issue had been retained by Eircom /Eircom Indigo under a statute which was the law of the land at the material time, and which prima facie required them to do so. Moreover, that domestic statute had been enacted to transpose, in part, Directive 2006/24/EC which also prima facie required them to do so. Moreover, the requests under s. 6(1) of the Act of 2011 made by the Chief Superintendents were also made before Directive 2006/24/EC had been impugned. In so far as both the service providers, and the Gardaí, were concerned, there was lawful authority for their actions. They were not to know that the legal uncertainty that subsequently developed would transpire. If, in retrospect, there is now serious doubt over whether their respective actions were in fact lawful, any illegal actions, or legally doubtful actions, by them must be regarded as having been unintended and inadvertent on their part, and not remotely culpable. The need to send a deterrent message would not arise in either case. Moreover, any technical illegality, or doubt as to legality, affecting the actions of Eircom / Eircom Indigo, and/or the Garda Chief Superintendents, that now exists would not have affected the fairness of the appellant's trial. Moreover, the public interest in admitting the evidence in support of the prosecution's case against the appellant would have far outweighed any countervailing considerations based on a need to be seen to be upholding EU legislative policy which was not patent at the time, although it was subsequently clarified in the two seminal judgments of the CJEU that post-dated the critical events in this case, namely the judgment in the *Digital Rights and Landesregierung* cases, and the judgment in the *Tele2 Sverige and Watson* cases.

127. We also agree with the trial judge's view that the appellant could have had no expectation of privacy while in the internet café on the 28th of September 2013 in the circumstances of the case. In so far as the emails sent on that occasion and on earlier occasions utilising hushmail email accounts were concerned, the only rights to privacy engaged, were those of the complainant and possibly those of the internet café owner. Moreover, it is well established (see *EMI Records (Ireland) Ltd v UPC Communications Ireland Ltd* [2010] 4 IR 349, *Idah v DPP* [2014] IECCA 3 and *People (DPP) v Kearney* [2015] IECA 64), and as Hogan *et al* in the 5th edition of *Kelly*: *The Irish Constitution* characterise it, "an unremarkable proposition", that the right to privacy cannot extend to participation in criminal activity. While the point must be taken that the evidence in this case does not establish that the appellant was engaged in criminal activity while in the internet café on the 28th of September 2013, the same cannot be said for the earlier occasions on which it is alleged she sent the various emails concerning the complainant.

128. In so far as the evidence obtained on foot of the mutual assistance request from Canada was concerned, there was simply no cogent evidence either that it was illegally obtained (in fact all of the evidence was to the contrary), or that it involved a breach of any of the appellant's rights. The admissibility challenge to that, and associated, evidence, and in particular the CD's, and the evidence of Steven Olaf Youngman and Darryl Krassman specifically referred to in ground of appeal no (ii), merited being dismissed *in limine*. We consider this challenge to have been completely untenable and bordering on unstateable.

129. For all these reasons we are not disposed to uphold grounds of appeal (i), (ii) or (iii).

Grounds (x), (xi), (xiii), (xiv) and (xvi) – Definition of Harassment

130. On day 13 of the trial, counsel for the appellant applied unsuccessfully for a direction on the harassment count, on the basis that the definition of harassment under s. 10 of the Act of 1997 did not include indirect communication of the type alleged by the prosecution in this case. It is suggested, *inter alia*, that the direction sought on this basis ought to have been granted.

131. The relevant subsections of s.10 of the Act of 1997 provide:

> 10.—(1) Any person who, without lawful authority or reasonable excuse, by any means including by use of the telephone, harasses another by persistently following, watching, pestering, besetting or communicating with him or her, shall be guilty of an offence.
>
> (2) For the purposes of this section a person harasses another where—
>
> (a) he or she, by his or her acts intentionally or recklessly, seriously interferes with the other's peace and privacy or causes alarm, distress or harm to the other, and
>
> (b) his or her acts are such that a reasonable person would realise that the acts would seriously interfere with the other's peace and privacy or cause alarm, distress or harm to the other.

132. It is accepted, and is uncontroversial, that s. 10(1) defines the behaviour that can amount to harassment as "following, watching, pestering, besetting or communicating". These terms are used disjunctively and thus any individual behaviour or combination of these behaviours can amount to harassment if they are performed "persistently", and they are done "intentionally or recklessly", and cause serious interference with another's "peace and privacy" or cause "alarm, distress or harm" to that other. Moreover, the list would appear to be exhaustive in that the behaviour complained of must fall into one, or more, of those categories if it is to amount to harassment.

133. The prosecution's case was that the harassment of the complainant was comprised by the following:

> 1. Letter sent to complainant's home in November 2011
>
> 2. Letter sent to DPP about complainant in March 2012
>
> 3. Leaflets placed on cars and pillars in her estate on 1st March 2012
>
> 4. Email sent to many recipients but not to the complainant from markkenny@hushmail.com on 31st March 2012
>
> 5. Letter sent to office of DPP on 21st April 2012
>
> 6. Email sent to many recipients but not to the complainant from johngilligan@hushmail.com on 1st June 2012
>
> 7. Email sent to many recipients but not to the complainant from clairefoley@hushmail.com on 4th August 2012
>
> 8. Two emails sent to many recipients but not to the complainant sent from brendanbarr@hushmail.com on 16th March 2013

134. The prosecution contended that the cumulative effect of the behaviour complained of was that the complainant was "beset on all sides" by the appellant, in that she found herself troubled by, in the sense of being surrounded by, and unable to get away from, the disparaging calumny and defamatory material being promulgated by the appellant. This was elaborated on by counsel for the respondent at the hearing of the appeal before us, as follows:

> "And can I submit to the Court, and I made this submission to the court below, that when you look at the totality of what was done in the case, giving "beset" its ordinary meaning but not as a term of legal art, giving it its normal meaning, the complainant in this case was beset. She was beset on all sides by what was done here and that, in my respectful submission, was the intention of the author. It was in her home, it was in her neighbourhood, when she went to work it was there, when she went to her doctor it was there, when she walked down the street she didn't know how many people she was walking past had read the information, meaning in this case, giving the word its ordinary meaning, was very much beset on all sides by the material that was disseminated. And that's giving the word its ordinary meaning but qualified, of course, by the threshold that the prosecution wasn't —
>
> MR JUSTICE EDWARDS: What do you mean when you say "beset on all sides"?
>
> MR NAIDOO: Hemmed in, surrounded by. She was surrounded by this information wherever she went; home, outside her front door, her place of work, her doctor, and then because the other emails were drawn to her attention she knew that any number of other people had also read the information. That's giving the word its ordinary meaning but not treating it in isolation and not treating it as a term of legal art with a limited meaning. The complainant in this case can properly be described as, as a matter of fact, having been beset by the material that was disseminated about her with the intention that it communicated to her and therefore the person is communicating with her in the same way that if I leave a message for Ms Justice Kennedy --
>
> MR JUSTICE EDWARDS: When you say hemmed in or surrounded, she couldn't get away from it.
>
> MR NAIDOO: She -
>
> MR JUSTICE EDWARDS: Sort of metaphorically but, I mean …
>
> MR NAIDOO: In my respectful submission, literally."

135. The case made by the appellant was that of the five forms of behaviour listed in s.10(1) of the Act of 1997 that could potentially constitute harassment (if the other conditions as to persistence, intention or recklessness, and consequences were satisfied), two of them, namely "watching" and "besetting", respectively, required to be treated as legal terms of art, and given the narrow legal meanings attributable to them in the Conspiracy and Protection of Property Act 1875 (the Act of 1875).

136. It is necessary to make a few observations on this. To "beset" as understood in Act of 1875 was interpreted as meaning occupying or surrounding a place – see *J Lyon & Sons v Wilkins* [1896] 1 Ch 811. To "watch" also had a meaning in that context, namely to spy upon or surveil a property, particularly at night (although not exclusively at night– see *Charnock v Court* [1899] 2 Ch 35) for illicit or sinister purposes. The natural and ordinary meaning of the word "watching" of course embraces the conduct just mentioned but also, more commonly, the entirely non-criminal activity of lawful surveillance of a property or thing, again particularly

at night, for protective purposes, and hence the term "night watchman", or a soldier or sailor being "on watch". (See also the word "watch" as discussed in Stroud's Judicial Dictionary, 5th Ed, where its usage in conjunction with the word "beset" is treated as analogous to its usage in conjunction with the word "ward", as in "watch and ward", in circumstances where Blackstone's Commentaries (1 Bl. Com 356) explain that "watch" is properly applicable to the night only whereas "ward" is applied to the daytime.) However, as it is used in the Act of 1875 to "watch" unquestionably attracts only the narrower and more restricted meaning of surveillance, particularly but not exclusively at night, for illicit or sinister purposes.

137. In modern times, when used as a legal term of art the two concepts under discussion are pleaded together but disjunctively as "watching or besetting", and they are primarily used in connection with trespasses to property, and very frequently in the industrial relations context where the complaint relates to unlawful picketing.

138. The respondent's case, however, is that there is no basis for treating the words "watching" and "besetting" as they appear in s.10(1) of the Act of 1995 as bearing anything other than those of their natural and ordinary meanings that relate to a potentially unlawful form of conduct. Although all five types of behaviour listed, namely "following, watching, pestering, besetting or communicating" are to be treated disjunctively, the order in which the words appear does not suggest an intention on the part of the Oireachtas that the words "watching" and "besetting" should be imbued with special legal meaning, and regarded as legal terms of art, while the other three words, namely "following", "pestering" and "communicating", should be given their natural and ordinary meanings. Arguably if the behaviours in question were to be confined to "watching" and "besetting" as legally understood one would have expected the two words to have appeared in the subsection either in the manner in which they are invariably pleaded, namely as "watching or besetting", alternatively beside each other in the list as "watching, besetting", but not separated by the word "pestering" as in fact occurs.

139. The prosecution firmly made their case on the basis that the conduct complained of came within the natural and ordinary meaning of the word(s) "besetting" or "to beset", and in support of that the trial judge was referred (without objection) to a definition from the Oxford online dictionary suggesting that the natural and ordinary meaning of besetting included "to trouble persistently."

140. Whatever about the Oxford online dictionary, and as pointed out the prosecution's recourse to it was not objected to, there is no doubt but that the print edition of the full Oxford English Dictionary (Clarendon Press: Oxford), now in 20 volumes, is a work of such renown and authority that a court could have no hesitation in taking judicial notice of it, and we do so. The second edition of this work, a copy of which we have access to in the Judge's library, suggests that there are three principal categories of meanings of the word "beset". These major categories are designated with the Roman numerals I., II., and III., and within each major category there are sub-categories of meaning designated by ordinary numerals, 1, 2, 3 etc.

141. The first major category is entitled: "*I. To set about, surround*". The second is entitled "*II, To set (in fig sense), to bestow*." The third is entitled "*III To become, suit*". The only major category of meaning of potential relevance in the present case is "*I. To set about, surround*".

142. Within that first major category, there are four subcategories, namely 1, 2, 3 and 4 respectively. Certain of these subcategories are in turn subdivided for the purposes of providing examples of the meanings contended for, with illustrations taken from usage of the word in literature, and each division is designated a, b, c, etc.

143. Subcategory 1 is entitled "*1. To set (a thing) about with accessories or appendages of any kind; to surround with things set in their places*". Amongst several illustrations of usage at "a" within this subcategory is a reference to "a diadem or tiara beset with pearls". More vaguely used it connotes "*To surround, encircle, cover round with*". Examples of this vaguer usage, provided at "b" within the subcategory, include references to "faces beset with sunbeams" and "angels beset with sunbeams". The second subcategory of meaning within this main category is "*2. To set or station themselves round, to surround with hostile intent*". Examples of how it has been used in this context include "*a. To set upon or assail on all sides (a person)*"; "b. *To invest, to surround (a place) to besiege*"; "*c. To occupy (a road, gate or passage), esp. so as to prevent anyone from passing", "d. To circumvent, entrap, catch*".

144. The third sub category of meaning within this major category is "*3. fig. To encompass, surround, assail, possess detrimentally*". The first example of such usage is "*a. said of temptations, dangers, difficulties, obstacles, evil influences*". A second is provided by "*b. of the difficulties, perils, obstacles which beset an action, work or course*". A third is provided by "*c. of actual enemies forming schemes against one's life or property*" and a fourth by "*d. To be possessed (with devils)*". The fourth, and final, subcategory of meaning within this major category is "*4. gen. To close round; to surround, hem in. (Often with some allusion to senses 2 and 3, as in 'to be beset by ice.')*."

145. The default rule of statutory interpretation is to afford words their natural and ordinary meaning, unless it is clear from the statute that they are to be afforded some special meaning and treated as a legal term of art. In this case we have considered s.10 of the Act of 1997 in detail. We have considered it first of all in isolation and in its own terms; then taking into account the part of the Act of 1997 in which it appears, we have further considered it in conjunction with the other provisions in that part and have had regard to its place in the scheme of the Act as a whole. Having done so, we are not satisfied that the word "beset" as used in s.10 is to be afforded any special meaning or that it is to be considered as a legal term of art.

146. The appellant has produced no authority for her contention to the contrary, beyond an opinion expressed by the author(s) of The Law Reform Commission's Issue Paper No 2 – Domestic Violence –Harassment (LRC IP 2-2013). While any opinion expressed by the Law Reform Commission is worthy of respect and due consideration, it is important to note that this document was neither a Consultation Paper nor a Report of the Law Reform Commission, merely an Issues Paper. It was intended to identify issues for discussion, not to indicate definitively any views of the Commission concerning how a statutory provision should be interpreted, or indeed as to the aetiology or provenance of such a provision. The document itself states that: *"[t]he purpose of an "Issues Paper" is to provide a summary or outline of a project on which the Commission is embarking or on which work is already underway, and to provide readers with an opportunity to express views and to make suggestions and comments on specific questions."* We feel that in the circumstances we ought to treat any views as to the law offered in such a document as the Commission's initial, tentative and provisional views only.

147. The particular comment relied upon by the appellant, which appears in paragraph 1.01 of that document, and which is to the effect that *"[t]he term 'besetting' derives from s. 7 of the Conspiracy and Protection of Property Act 1875 and has been interpreted as meaning occupying or surrounding a place*" was offered as part of a description of s.10 as a prelude to asking the question: "*Q.1: Do you agree that the current definition of harassment in section 10 of the Non-Fatal Offences Against the Person Act 1997 is sufficiently broad to include the types of harassment, such as stalking, that are common in a domestic violence setting?*" For

completeness, we should mention that there are two footnote references accompanying the sentence relied upon by the appellant, the first of which (fn 10) points out that "[*s*]*ection 7 of the 1875 Act set out the offence of unlawful intimidation which included where a person 'watches or besets' another person. S.7 of the 1875 Act was replaced by section 9 of the 1997 Act, which provides for the offence of unlawful coercion and which also includes where a person 'watches or besets' another person*"; and the second of which (fn 11) refers the reader to the case of *J Lyon & Sons v Wilkins* cited earlier in this judgment. We have taken account of these references in arriving at our view.

148. More significantly, although we were not referred to it by counsel, the actual Law Reform Commission Report that followed on from research conducted by the Commission subsequent to responses having been received to the said Issues Paper, namely, it's Report on Aspects of Domestic Violence (LRC 111-2013), confined itself to suggesting that the current definition of harassing behaviour was insufficient to capture certain types of indirect harassing behaviour such as where the behaviour of the defendant is directed towards a person other than the complainant but concerning the complainant, for example where the defendant spreads harmful information, whether true or false, about the complainant to the complainant's friends and family. The Law Reform Commission specifically drew attention to the English case of R. v Debnath [2005] EWCA Crim 3472, and commented "*[t]he Commission is not aware of a case with similar facts having been prosecuted in Ireland but it would appear that this type of conduct would not breach section 10 because it would not amount to any of the terms 'following, watching, pestering, besetting or communicating with' the complainant*."

149. In *R. v Debnath* the defendant pleaded guilty to harassment pursuant to section 2 of the (English) Protection from Harassment Act 1997. The defendant and the complainant had a one night stand after which the defendant mistakenly believed she had contracted a sexually transmitted disease. This sparked a year-long campaign by her of harassing the complainant, mainly through online means. This included sending the complainant's fiancée emails claiming to be from one of the complainant's friends detailing alleged sexual indiscretions and sending the complainant's former employers an email, also claiming to be from him, which falsely alleged that the complainant had harassed the defendant. The defendant also registered the complainant on a database for individuals with sexually transmitted diseases seeking sexual liaisons, and on a gay American prisoner exchange, and set up a website claiming that the complainant was gay.

150. In its Report on Aspects of Domestic Violence 2013 the Commission stated, at para 2.16, that they were "*not aware of a case with similar facts having been prosecuted in Ireland but it would appear that this type of conduct would not breach section 10 because it would not amount to any of the terms 'following, watching, pestering, besetting or communicating with' the complainant*."

151. The Commission returned to this subject, and re-iterated the views just recounted, in its Report on Harmful Communications and Digital Safety 2016 (LRC 116-2016) at para 2.35. However, there was no specific discussion in either the 2013 or 2016 reports of whether the word "beset" is to be treated as a term of art and afforded the narrow meaning attributable to it under the Conspiracy and Protection of Property Act 1875, or those of its wider natural and ordinary meanings which could potentially constitute unlawful conduct. Moreover, the 2016 report, at para 2.37, having noted newspaper accounts of two first instance prosecutions under s. 10 of the Act of 1997, observes: "*[t]hese cases suggest that there is a view that section 10 may extend to some situations where a person is exposed indirectly to publicly available content. So, just as persistently displaying abusive placards about a person in public places might amount to traditional harassment, in the online context posting abusive content on publicly accessible websites or social media profiles might amount to online harassment. However, both of these cases involved guilty pleas and so the law in this area has not been properly tested.*"

152. In the present case counsel for the respondent made, and has reiterated before us, the case that what the appellant is contending for, in effect, is that the word "directly" should be implied into s. 10(1) immediately before the five potential forms of harassment that are listed. However, he submits, there is simply no legal basis for doing so. We agree with him.

153. When the issue was canvassed before the trial judge, she ruled as follows:

> "*Mr O'Higgins maintains that the Law Reform Commission itself did not contemplate the application of the term "besetting" to indirect third party communications and, therefore, the Court should not. He maintains that the Court should apply the meaning accorded to besetting in the Law Reform Commission on domestic violence. In deciding the meaning to be attributed to terms used in statutes, the courts have traditionally looked, first, to the definition contained within the text of the statute itself. Failing that, the Court looks for guidance for any definition contained in other relevant legislation. The Supreme Court's decision in the Minister for Justice Equality and Law Reform v. Donnelly and the DPP v. Brown, Court of Appeal 7th of December 2016, demonstrate that the Court should adopt the ordinary natural meaning of terms and, where appropriate, apply the dictionary meaning of a term. This was done in circumstances where the Non-Fatal Offences Against the Person Act itself provided a definition of a sort. In consulting the dictionary definition, the courts have demonstrated a preference for the Oxford Dictionary of English. The 2017 version of the Oxford Dictionary defines "pestering" as troubling or annoying someone with frequent or persistent requests or interruptions. Pestering is, therefore, not applicable to the facts of this case.*
>
> *To beset is defined as to trouble (someone or something persistently). In my view, it is open to the jury to conclude that evidence of sending emails to virtually every major public body in the state, to the editors of major national newspapers, to public relations companies, to a general practitioner, among many others, is evidence of persistent acts intended to trouble [the complainant]. The volume of emails sent and the breadth of its circulation was such that the emails could not have escaped her attention and the jury would be entitled to infer that this was the intention of the sender. The evidence of receipt given by a number of the recipients of the respective emails is such that the Court is entitled to reasonably infer that the email was both sent and received. In view of the evidence given by [the complainant] as to the effect of the circulation of each individual email on her, I have no difficulty in concluding that [the complainant] was beset by the sending of these emails and the other documents. Therefore, the accused has a case to answer in respect of all three counts.*"

154. We consider that the trial judge was entirely correct in how she dealt with this issue, and we find no error of principle. She was correct to reject the complaint made, and to refuse the direction sought, on the basis that the behaviours complained of could not potentially come within the meaning of "besetting" as it is used in s.10(1) of the Act of 1997, namely within the natural and ordinary meanings of that word. Her approach to the correct interpretation of the statute was impeccable and entirely in accordance with the law in our view. We therefore reject grounds of appeal no's (x), (xiii) and (xiv).

155. Grounds (xi) and (xii) were not canvassed in oral argument at the hearing of the appeal, but neither were they abandoned with the appellant's counsel being content to rely upon the written submissions filed. In essence they boil down to a contention that the

prosecution ought not to have been allowed to rely on certain of the defamatory documents that were promulgated as being "communications" with the complainant in circumstances where they had been sent or addressed to third parties, or "to whom it may concern", rather than directly to the complainant; alternatively where they had simply left in public places unaddressed to any specific person or persons, for example leaflets/posters placed on the windscreens of parked cars or pinned/stuck on to street poles or other structures in public spaces.

156. The trial judge's ruling on this aspect of the case was as follows:

> *"In respect of count No. 1, an argument has been made that the communications, with the exception of L1, do not amount to harassment because they do not fall within the defined categories of conduct specified in section 10(1), namely, watching, besetting, pestering and communicating with the person affected. It is accepted that to satisfy the requirement of persistence more than a single instance of communicating with a target is required. In the alternative, a single instance of communicating with a target might be combined with instances of pestering or besetting, if the evidence establishes that there are one or more instances of pestering or besetting.*
>
> *It has been submitted that, in order to communicate with another person, it is necessary that the communication be addressed to or direct to that person, even in circumstances where one of the letters was sent to* [the complainant's] *place of work and was circulated for general consumption, as was connoted by the salutation "To whom it may concern". It is submitted that the fact that the letter to the office of the DPP is about* [the complainant] *and not addressed to her implies that it was not intended for her eyes and, consequently, does not constitute a communication with her. Similarly, it is submitted that the leaflets which were posted all over her neighbourhood for all to see, including the complainant] herself, were not communications with her.*
>
> *In my view, these two items were capable of constituting communications with* [the complainant] *because they were manifestly intended for her eyes, which is why they were sent to a place or left at a place where she would, absolutely without a doubt, receive and read them. It is the prosecution case that the communications were maliciously intended to interfere with her peace of mind. This end could not have been achieved if she had no knowledge of their existence. It is open to the jury to infer that these communications were circulated in these two venues specifically so* [the complainant] *would get to know of them and read them, and this is what in fact occurred and the content caused her some considerable distress.*
>
> *Communicating with someone involves imparting information to that person or the expression of one's views, beliefs or opinions on any subject, including the target of the communication. This objective was achieved by the author of the items sent to the DPP's office and the leaflets. Even if I am wrong in that, the prosecution maintained that all of the documentation sent by email or otherwise, and including the aforementioned documents, fall within the category of pestering or besetting* [the complainant]*."*

157. We consider that the trial judge's approach to this issue was common sense and impeccable, and we have no hesitation in upholding her ruling as having been correct. Moreover, in so far as she suggested that there were available inferences that might be drawn by the jury, there was certainly evidence that would allow those inferences to be drawn were the jury so minded. We find no error of principle.

158. The final ground of appeal in this group is ground no (xvi). Again, this was the subject of written submissions only, but has not been abandoned. It was complained that the trial judge erred in law and in principle in her charge to the jury in saying that to convict of the harassment that they did not need to be satisfied that the appellant had committed all the acts alleged.

159. The context in which this complaint arises is evident from the following extract from the trial judge's charge to the jury, in which the trial judge was explaining to the jury the ingredients of the crime of harassment as framed in s.10 of the Act of 1997:

> *"The last element is that the acts complained of, "intentionally or recklessly, seriously interferes with the other's peace and privacy or causes alarm, distress or harm to the other, and (b) his or her acts are such that a reasonable person would realise that the acts would seriously interfere with the other's peace and privacy or cause alarm, distress or harm to the other." Now, that requirement speaks for itself. In order for you to convict, you must be satisfied beyond reasonable doubt that [the complainant's] peace and privacy were seriously interfered with or that she was caused either alarm, distress or harm and that this was the intention of the sender or that the sender was reckless as to the effect the communications would have on [the complainant]. So in assessing the evidence in relation to the harassment count, you must consider whether all of the elements of the offence have been established, the first being was Eve Doherty the author of some or all of the communications and if she was, is persistence established by reference to that number?*

160. In the written submissions the complaint is framed in terms that:

> *"where the prosecution case was opened and closed on the basis that the appellant had sent all eight communications, for the jury to be then told that they only had to be satisfied that she sent more than one of the communications provided they were satisfied as to persistence was incorrect. While it is accepted that the trial judge in her charge told the jury that they must decide the facts on the basis of a unanimous verdict, it is submitted that it is unclear as to on what the factual basis the jury convicted the appellant."*

161. In support of this submission we were referred to a passage from the judgement of the Court of Criminal Appeal in *The People (Director of Public Prosecutions) v.M.R* [2010] 1 IR 577, the facts of which were very different to those in the present case. We do not see it as being very much in point. Be that as it may, it was submitted that the critical foundation to a verdict of guilty was absent in the present case, as the jury had been told that they could find the appellant guilty of harassment if they found that the appellant had committed just two of the acts alleged. The question was posed, rhetorically, "how can the court sentence an appellant when it is unclear as to what acts have been committed that form part of the offence?".

162. Just dealing with the rhetorical question in the first instance, it is very largely answered by the approach commended by the Supreme Court in its recent decision in the case of *The People (Director of Public Prosecutions) v. Mahon* [2019] IESC 24, where Charlton J stated:

> "Where there is an ambiguity in the factual implications of the jury's verdict, the judge is entitled to come to an independent conclusion as to the relevant facts upon a consideration of all of the evidence presented before the jury.

> Any such fact must be found only if the trial judge considers that it has been proven beyond reasonable doubt during the course of the trial."

163. In any event, we do not consider that the trial judge was in error in leaving the matter to the jury in the manner that she did. It was submitted by counsel for the prosecution in his replying written submissions that if the judge had told the jury that without a finding that all the communications were sent by the accused they could not go on to consider the second aspect of the ingredients to the offence, she would have been usurping their function. We do not consider that it is necessary to express a definite view on this. Neither would we foreclose on the possibility that there might be other ways of dealing with the hypothetical issue raised. Be that as it may, we are completely satisfied that in the overall context of the issues that the jury were required to consider, and having regard to the evidence before them, and the general run of the case, the trial judge's instruction was unobjectionable and did not represent an error. As a significantly ambiguous guilty verdict was no more than a highly theoretical and, in our view, quite remote possibility on the run of the case, we do not consider that specific action was required to guard against it in the circumstances facing the trial judge, and we do not regard the trial judge's actual instruction to the jury as having been either legally incorrect or a misdirection at any level. Were a serious concern as to what acts underpinned a guilty verdict to have arisen, it was capable of being dealt at sentencing by means of the judge coming to an independent conclusion as to the relevant facts upon a consideration of all the evidence presented before the jury. We have before us the transcript of the sentencing hearing and consider it relevant that at no point was it suggested that the verdict of the jury had been ambiguous or that there was any uncertainty as to the evidential basis for the appellant's conviction.

164. In the circumstances we also dismiss ground of appeal no (xvi).

Grounds (v), (vi) and (vii) – Absence of evidence that certain documents were written by the appellant.
165. The prosecution sought to draw evidence of comparison between certain handwritten and typed documents obtained during a search of the appellant's home, certain typed documents found in the appellant's locker in work and other documents, particularly the eight "communications" which prosecution said amounted to harassment. The purpose of this exercise was to try and persuade the jury that the appellant was the author of the eight communications.

166. It was submitted to the trial judge by defence counsel on day 9 of the trial that in circumstances where the prosecution was not in a position to prove that the appellant had written the documents found in her house and locker, that these documents should have been excluded for the purpose of a comparison. The prosecution contended that the documents recovered from the appellant's house were real evidence that the jury should be entitled to receive and scrutinise. The defence contended that that was an incorrect characterisation in so far as notations on the documents were concerned. It was submitted that any notations on them were hearsay, and thus did not assist the prosecution in proving the provenance of the writing thereon.

167. The trial judge ruled the evidence admissible, stating:

> *"I am of the view that the items of handwriting material or at least the letters found at the accused's own home fall on the right side of the distinction between hearsay and real evidence and I am satisfied that it is real evidence."*

168. The respective positions of the parties were reprised in the written submissions filed before this court, and there was only brief reference to them during oral submissions before us. However, it is of significance that it was acknowledged by counsel for the appellant at the hearing of the appeal that there had been discussion in the court below concerning whether the rule against hearsay has any application to statements comprising real evidence, which the prosecution were contending this was, or for that matter original evidence whose evidential value lies in the fact that a statement was made, regardless of whether or not it is true – the classic example being evidence of a libel - as opposed to testimonial evidence in which the party adducing it intends to rely on the truth of its contents. That is really the nub of the matter as far as we are concerned. The rule against hearsay has no application to statements in writing, in whatever form it is sought to introduce them, be that as real evidence or as original evidence, where reliance is not being placed on the truth of the contents of the document. The prosecution was not relying on the truth of the contents of any of these statements, whether that be principal content or notations added thereto. If, for example, one of the documents had purported to bear the signature of the appellant, and the prosecution were contending that it was a true signature, that would be an entirely different matter. However, the prosecution simply wished to establish as a matter of circumstantial evidence that documents bearing certain handwriting, and typescript, were found in places which were private to, or largely private to, to the appellant, such as her home and her locker. Of course, the hope was that this circumstantial evidence, combined with other circumstantial evidence in the case, would in due course be sufficient for a jury to draw an inference as to the authorship of the allegedly harassing documents that were promulgated. That was an entirely legitimate exercise.

169. Counsel for the appellant's argument, as made to the trial judge, appears to us to have conflated the separate issues of the need to establish authenticity and authorship of a document by proving due execution and content, where it is proposed to put it in evidence on an attributable basis, on the one hand; and a document's legal admissibility on the other hand. The prosecution was not seeking to attribute these documents to the appellant solely on the basis that they were found where they were found, and/or on the basis of their manifest physical and visual features, including the statements contained thereon. They were merely being introduced, on an initially unattributable basis, as pieces of circumstantial evidence. As already alluded to, it was undoubtedly hoped, and it was part of the prosecution's legitimate legal strategy, that they would be able to suggest to the jury at a later stage that, by combining the real evidence then at issue with other evidence in the case, they could draw their own inferences as to attribution.

170. In our view the trial judge's ruling was correct. The rule against hearsay had no application. As the prosecution were not, at the point of introducing the evidence, affording it any specific attribution beyond the fact that it was found on a certain occasion in a certain place, no further evidence as to authenticity and authorship was required. The fact that the prosecution had introduced the evidence without specific attribution was something that defence counsel could comment upon in his speech if he felt it was appropriate to do so. In that regard, we note the query raised by the trial judge when the issue was being canvassed before her in the absence of the jury: "*Does that not just go to weight, though, Mr O'Higgins*." In suggesting that, the trial judge had an entirely correct understanding of the position in law in our view.

171. In the circumstances we are not disposed to uphold grounds of appeal no's (vi) and (vii).

Ground (iv) – Alleged breach of rights to privacy.
172. The complaint here relates to the introduction in evidence of the e-mail sent concerning Commissioner Callinan on the 28th of September 2013. The appellant's point is that in sending this e-mail she was not committing any criminal offence and that she had an expectation that her rights to privacy, deriving from various sources including the Constitution, the Charter and the ECHR, in respect of e-mails sent by her, even from a public place such as an internet café, would be respected. In the circumstances where she contends that her said rights to privacy were violated, her case is that evidence concerning the circumstances in which the said was

sent should have been excluded. A hard copy of the e-mail introduced at trial had been procured from one its recipients, and accordingly was not directly the result of any breach of privacy. However, evidence as to the circumstances in which it was sent, and as to the means by which it became known about, and to whom it had been addressed, arose as a result of the viewing of the e-mail in question by Mr Babu Kandra on his terminal in the internet café at the time that it was being created, and subsequently by Detective Garda AR who had photographed a "screen grab" of what was visible concerning the e-mail on Mr Kandra's terminal.

173. The prosecution has argued that the appellant's rights to privacy are not absolute, and they must yield in appropriate circumstances to the public interest in the investigation of crime. Although the sending of this e-mail was not itself a crime, the e-mail in question was nevertheless highly material to an active criminal investigation, in circumstances where the appellant was the principal suspect in that investigation, and it was recovered in the course of that investigation. Moreover, given the ephemeral nature of the digital record and its potential relevance, urgent steps were required to note and record its contents lest it be erased. It is highly significant in our view that when the hard drive on terminal 15 was seized by gardai and technically examined it was found to have been wiped or erased by the appellant. Fortunately, however, there remained the records created by Mr Kandra and Detective Garda AR.

174. The trial judge considered the submissions on the issue and ruled:

> *"JUDGE: Now, this is an application to exclude two items of evidence both gathered at the Wired Internet Café on Aungier Street on the 28th of September 2013. The basis upon which it is sought to exclude the evidence is that the manner in which the evidence was obtained constituted an unjustified interference with the accused's constitutional right to privacy. For the purpose of this ruling I heard evidence from Babu Kandru the proprietor of the café and the Garda AR a member of the National Surveillance Unit both of whom detailed the circumstances under which they obtained the respective items of evidence. During the course of the trial the scope of the right to privacy has been ventilated at length and it is acknowledged that the degree to which the right must be respected depends on the circumstances under which it is being exercised and the purpose for which the privacy is being sought. There is an absolute right to privacy for persons engaged in particular activities in particular locations on one hand and there is no right of privacy for someone who is secretly committing a criminal offence on the other. However there is a wide spectrum and the exercise in which the Court is engaged is locating where on the spectrum the right to privacy lies in these particular circumstances.*
>
> *I have made a previous ruling in this case which had at its heart an assessment of the reasonable expectation of privacy a person would hold in respect of the presence of a garda surveillance camera in a public internet café. Equally this ruling requires an objective assessment of what was reasonable expectation in the circumstances outlined by Mr Kandru. Two points have been highlighted by Mr O'Higgins in this regard. The first being that there is no suggestion that the accused was doing any unlawful act in the café on the 28th of September. The second point highlighted is that the right to privacy extends not only to the content of communications but also to the right of the author of the communications to remain anonymous. He identified the particular instances where it is manifestly in the public interest to respect the right of the author to remain anonymous such as whistle blowers, police informers and so on. The email being communicated on this occasion does not fall comfortably into that classification. However, the basic premise of the communication was a matter of very considerable public interest. On any analysis it is simply not tenable to suggest that the author of the email intended the content of the email to remain private therefore this ruling is limited to a consideration of whether the accused's right to privacy encompassed a right to communicate anonymously and the degree to which that right must be respected. In assessing Mr Kandru's actions it is of some considerable significance that Mr Kandru was aware that the accused was someone of interest to the gardaí. From that point onwards it was incumbent on Mr Kandru to ensure that his own commercial interests were secondary to his responsibilities to the community. It is also of significance and a source of some reassurance that the café has the facility to monitor the content of patrons activities should the need arise. It is of equal reassurance that it is not a facility that is employed by him on an indiscriminate basis. It is apparent from Mr Kandru's actions that he considered the need to employ that facility arose on this occasion. This was a responsible approach in my view. What he observed was of such concern to him that he made a record of it and he called the gardaí which again was a responsible response to the situation. This leads to the evidence of Garda R who came to the internet café by invitation and who was shown the content of the accused's monitor by Mr Kandru and who duly took photographs. At the point when the photographs were taken the accused was someone who was under active investigation and it would be absurd to suggest that she enjoyed the same right to privacy as the other internet café users who were going about their business privately and without encroachment. It would be equally absurd for Garda R to have ignored the evidence under his nose and to have instead sought to exercise the coercive garda power to achieve the same result. The fact that the accused wiped the c: drive leaving no trace of the email of itself demonstrates why the course adopted by Garda R was the sensible and correct course. In short because the accused was a person who was under active investigation by the gardaí at the time these items were obtained her right to privacy was severely curtailed. As it was nothing inherently unlawful in the actions that Mr Kandru or Garda R I am ruling the two items of evidence are admissible."*

175. In our judgment the trial judge was entirely correct to admit the evidence. We share her view that as a matter of common sense the appellants rights to privacy were severely curtailed in the circumstances of the case. Moreover, we are satisfied that the actions of Mr Kandru, who was aware of the Garda investigation, and specifically of the Gardai's interest in the appellant, and those of Detective Garda R, to the extent that they interfered with the appellant's rights, were not in any way disproportionate having regard to the legitimate aim then being pursued. We do not believe in the circumstances that the appellant's rights to privacy were unlawfully interfered with. In our view the trial judge was right to admit the evidence. That is our decision. However, we would add that even if there we are wrong about this, this was manifestly a case in which the trial judge would have been entitled to admit the evidence in any event on the basis of *The People (Director of Public Prosecutions) v J.C.*. Strong evidence based excusatory circumstances clearly existed, and these would justify the exercise of the discretion to admit the evidence in controversy in any event.

176. We are not therefore disposed to uphold ground of appeal no (iv).

Ground (viii) – Issues arising from presentations by non-expert witnesses.

177. This ground is pleaded in terms that the trial judge erred in law and in principle in failing to exclude the evidence of Suzanne Lindsay and Sarah Skedd and in allowing copies of the presentations created by those witnesses to be given to the jury. Before considering the challenge to the admissibility of their testimony, it is necessary to outline who these witnesses were, the circumstances in which they came to be asked to testify, and the nature of the evidence that they could provide.

178. Sarah Skedd was a Garda officer attached to An Garda Siochána's analyst service at the Special Crime Operations Unit in

Harcourt Square, Dublin 2. She was not proffered as an expert witness, and she did not purport to offer opinion evidence by way of expert testimony. Rather, she had been tasked to organise, collate, compare and highlight certain features evident in some of the documentary exhibits to be put before the jury, for ease of presentation of the evidence by the lawyers in the case and ease of assimilation of that evidence by the jury. In organisational terms her task was essentially clerical in that it involved collating and recording salient details concerning relevant exhibits in spreadsheet format using Excel software, for ease of later comparison of the actual exhibits and cross referencing by interested parties. The exhibits she was concerned with were those providing details of relevant e-mails allegedly sent by the appellant using various hushmail accounts, some of which had been sent to hundreds of recipients. In layman's terms she built a roadmap to facilitate persons involved in the trial, including the judge, counsel, witnesses and the jury, to quickly locate and view certain features to be seen in those documentary exhibits and on which the prosecution were placing some reliance as circumstantial evidence. Features highlighted on her spreadsheet included essential details about each document such as the date and time of sending of an e-mail, the e-mail account used, the intended recipients to whom the email was addressed, recipients in common with other e-mails, and matters of that sort. The evidence to be given by the witness, and in fact given by her, was simply a description of the task she performed, and presentation and where necessary explanation of the 50 page spreadsheet that she created. She was not cross-examined.

179. Suzanne Lindsey was a civilian working with An Garda Siochána. She carried out two comparison exercises, broadly similar to that carried out by Garda Skedd, in respect of several of the key documentary exhibits, to highlight commonalities and similarities in the language used in those documents. When she gave her evidence, she explained that she was looking for common spelling and punctuation mistakes, commonalities in formatting, punctuation and syntax, commonalities in the use of particular phrases, commonalities in the use of particular words, commonalities in the use of swear words or insults, and commonalities in allegations or claims made. She considered the documents in two separate groups, namely the eight documents concerning the complainant which were specifically being relied upon as representing harassing material as a first group, and then "other documents" including the e-mail concerning Commissioner Callinan, the documents seized at the appellant's home and those found in her locker, as a second group. Ms Lindsey did not prepare a spreadsheet but had prepared a report, although at no stage was it sought to introduce her actual report in evidence. Rather, she merely gave lengthy viva voce evidence concerning what she had taken note of during her comparisons. Then, with the specific leave of the trial judge, she produced an A3 sheet summarising the extent of the commonalities and similarities that she had noted, for the assistance of interested parties including the jury and the jury received a copy of this. As in the case of Ms Skedd, Ms Lindsey she did not purport to testify as an expert. She asserted no special skill or knowledge. Her task had essentially involved laborious and meticulous but unskilled comparison of relevant documents to identify features of the types indicated if such existed, the reporting on and highlighting through testimony of any such features identified, and the presentation of a summary of what the comparison exercised had revealed in an organised and easily understandable format.

180. The evidence of these witnesses was objected to on the basis that "it was unfair on the appellant to try to make the evidence more palatable by calling a witness who was not an expert" It was further submitted that there was a risk that the jury's function would be usurped by these witnesses and that more significance would be attached to the documentary evidence than was deserved.

181. These arguments were rejected by the trial judge, who ruled as follows:

> *"JUDGE: All right. Very good. I've considered the submissions made in relation to the admissibility of the evidence of Suzanne Lindsay and Ms Skedd and in my view, there is no sustainable objection to the content of Ms Linsday's report. I am of the view that the items of handwriting material or at least the letters found at the accused's own home fall on the right side of the distinction between hearsay and real evidence and I am satisfied that it is real evidence. The remaining objection to Ms Lindsay's evidence is based on a perception or a possible perception by the jury that it is some form of superior evidence because it's presented in the manner in which it is and I believe that's a matter which can adequately be addressed in my directions to the jury and 1 don't believe that there's any real force to the objection to the evidence to be given by Ms Skedd and I'm of the view that that also should be admitted."*

182. We regard the objection to the testimony of these witnesses as bordering on the unstateable. We are completely satisfied that there was no unfairness in presenting information gleaned during extensive comparative exercises in an organised and easily manageable way. Both the spreadsheet and the summary sheet prepared by these witnesses merely facilitated presentation of the evidence. It did not alter it, or embellish it, in any substantive way. It simply organised it and presented it in a format that made it easier to understand and assimilate. There was nothing remotely unfair in that.

183. We are not there disposed to uphold ground of appeal no (viii)

Ground (ix) – Refusal to direct the false statement counts.

184. While it was accepted that the jury ultimately acquitted the appellant of the two counts on the indictment relating to the making of a false statement, it was submitted that the learned trial judge erred in failing to direct an acquittal in respect of these counts and that to leave them to the jury was prejudicial and unfair in the circumstances of the case. It was implicit in this argument that doing so somehow operated to adversely influence the jury to bring the guilty verdict on the harassment count that they did.

185. Section 12 of the Criminal Law Act 1976 provides that:

"Any person who –

> (a) knowingly makes a false report or statement tending to show that an offence has been committed, whether by himself or another person, or tending to give rise to apprehension for the safety of persons or property […]

shall be guilty of an offence"

186. The prosecution case was that in respect of the poster and one of the emails, which both contained an allegation that the complainant had perverted the course of justice by interfering in the prosecution of a drugs matter related to a neighbour, that these were both false statements tending to show that an offence had been committed.

187. It was submitted that the legislation was directed at persons who knowingly made false statements to members of An Garda Síochána, and was never intended to capture the situation at issue where a person alleged to someone else that another person had committed a criminal offence. In those circumstances, it was submitted, the counts relating to the making of a false statement should never have been allowed to go to the jury.

188. In response to this counsel for the respondent contends that the trial judge was correct not to withdraw this case from the jury. The jury gave careful consideration to the issues raised by the appellant in that regard and assessed the evidence in that light.

Ultimately it was for a jury to decide on the facts of the case and as to whether the charges had been proven.

189. While the appellant has submitted that the legislation was never intended to capture the situation at issue where a person alleges to someone other than An Garda Siochána that another person has committed a criminal offence, no such limitation is apparent in the wording of the section which creates the offence, nor is it a requirement of same that the report or statement should be made any particular person or organisation.

190. We find ourselves in complete agreement with counsel for the respondent and we are not therefore disposed to uphold group of appeal no (ix).

Ground (xv) – The closing speech.
191. The final ground of appeal canvassed in respect of the appellant's conviction complains that the trial judge erred in law and in principle in refusing to discharge the jury where prosecuting counsel in his closing speech placed emphasis on a document being found on a scanner with a separate header which had not been adduced in evidence, or any attention drawn to this during the evidence, to the court or to the defence, and the learned trial judge erred in law and in principle in telling the jury to ignore this aspect of the prosecution's closing speech.

192. The background to this complaint is to be found in the evidence of Suzanne Lindsey. While giving evidence of her comparison exercise, in the course of which she had compared the documents seized at the appellant's home with other documents, she spoke about features she had noted on two of those documents, namely WH 9 and WH10, respectively, which purported to be documents addressed to the appellant. In considering the formatting of these documents, which was one of her criteria for comparison purposes, she had noted something odd about WH9. However, she did not mention it in her evidence in chief. This, it may be inferred was because, as she explained while being cross-examined, she was only concerned to record matters that qualified as a commonality in terms of her criteria. Indeed, when summarizing her findings, her evidence had simply been that "WH 9 contained 10, and WH10 contained zero" (of the commonality features she was looking for).

193. Of further relevance is the fact that she had also considered another document in the same group, TMC 12A which was in two physical parts. These two parts had been found together, but loose and not attached in any way, on the glass plate of a computer document scanner during the search of the appellant's home. The parts consisted of a document header which was in fact taken from an official Garda letterhead, and a sheet with a typed content that was without its own header. The separate "Garda" document header was positioned in the place where if the sheet with typed content had had its own header that header would have been.

194. There are several details of importance with respect to TCM 12A that subsequently emerged. The first is that WH9 was ostensibly a copy of the documents comprising TMC 12A married together so that they appeared as one document. Secondly, the defence, although they could have done so, never inspected the original exhibit TCM12A, and had not appreciated that it was in two parts. Thirdly, the exhibits list had referred to TCM 12 A as being "a document". Fourthly, the copy of TCM12A which the defence had received in disclosure had again ostensibly married the two parts together so that, on a cursory inspection, it appeared to be comprised of a single sheet. Fifthly, the odd feature of WH 9 that had been observed by Ms Lindsey, but not mentioned by her during her evidence in chief, was that the Garda logo and accompanying text in the document header appeared to be slightly off-centre.

195. While she was being cross-examined about TCM 12A it was put to Ms Lindsey that it was a typed letter, which was obtained from a scanner or a printer in the appellant's house. She responded: "*Yes, it looked like a draft, the beginning of a draft letter and also the headed — from what I can recollect the headed paper I think was detached, was separate, had been stuck on the garda headed paper*." Defence counsel did not appear initially to appreciate the import of what was being said, and continued to probe the nature of similarities that had been spoken of earlier by the witness, putting it that rather than there having been true similarities resulting from the same mistake having been made on more than one occasion, there had merely been a "transposition" of a once off mistake by virtue of some cutting and pasting in the creation of the documents being compared.

196. The cross examination then moved on, and WH9 was called for and was placed in the hands of the witness. She was asked to confirm that it was a letter written on Garda note paper. To that came the following in response:

> *"A. It appears to be. It's slightly off centre. Having worked in the guards for nine years, the logo is normally slightly to the left so it doesn't look like a correct logo to me.*
>
> *Q. Yes, it's not dead centre?*
>
> *A. Yes."*

197. The cross examination then moved on to a consideration of the content of the document and evidence was elicited, *inter alia*, that it purported to be a letter written to the appellant in disparaging terms. The prosecution sought to make the case that the appellant had in fact written this letter, and WH10, to herself in effect to lay a false trail by painting herself as a further victim of an unknown harasser in case she was suspected of being the person who had promulgated the offensive material about other persons including the complainant.

198. The issue the subject matter of this ground of appeal arises because following Ms Lindsey's evidence, in circumstances where she was the last witness for the prosecution, and where following an unsuccessful application for a direction, the defence had indicated they were not going into evidence, the trial moved immediately into its next phase, namely closing speeches to the jury. The complaint centres on the following remarks of prosecuting counsel during his closing:

> *"Of course, again it is possible that a person other than the accused wrote both of those documents, but is it a reasonable possibility? It would require that a different person wrote the two documents, put her name on one of them, and left them in her house. Two of them, WH 9 and WH 10, it is suggested were not written by her. That is suggested because they were found in her place of work and they appeared to have been addressed to her and they were abusive of her and the suggestion therefore is made that that means she did not write them and if they compare to other documents that are part of the harassment, that means that she didn't necessarily write those either. A quick look at that. First of all, there's the document itself. This is a copy of WH 9. You have heard from Suzanne Lindsay. She was in the gardaí for years and years and years and she pointed out that the header on it isn't centred; it's off centre. Well, so what? Well, let's have a look at TMC 12-A, the original. This is the typed letter found on the scanner in the accused's home and that is how it was found, with the header separate from the letter on the scanner. So what it looks like is that Ms Doherty, in the privacy of her own home, was making the letter look as though it came from the gardaí by grafting the garda logo onto the top of it, which, according to Ms Lindsay is what may have happened here, so again an unusual*

thing to do and a striking similarity."

199. We are told that at this point the exhibits officer walked in front of the jury holding the relevant exhibits.

200. The complaint is made that at no stage prior to counsel's closing speech had the case been made that the appellant in the privacy of her home was making a letter look like it came from the An Garda Síochána by grafting the garda logo on to it. Moreover, it was submitted, despite what was said by counsel for the prosecution in his closing speech, Suzanne Lindsay did not at any stage offer, in terms, the view that the appellant had grafted the garda logo onto WH9.

201. An application was made for a discharge which was refused by the learned trial judge, although she charged the jury in the following terms:

> *"I want you to be a little bit careful in relation to that particular evidence because the evidence given by Garda Lindsay was linked in the closing speech by the prosecution to the finding of a document and a header on the scanner in Ms Doherty's house. And it wasn't apparent at the time that Ms Lindsay was being cross-examined that in fact the header was separate from the document and she wasn't cross-examined in relation to that element of things at all. And the prosecution are now attaching a significance to that fact that Ms Lindsay said that the header on the letter was off-centre and that there was a piece of paper that would have assisted somebody in doing that if they were so minded. The prosecution are making something of that now. I think, in fairness, because Ms Lindsay wasn't cross-examined in relation to that at all, that that's not a part of the evidence that you should attach excessive significance to. I think that is out of fairness to the accused.*

202. The appellant's case, in substance, was that the way the trial judge dealt with it was not adequate to meet the situation, and that she had been wrong not to discharge the jury.

203. We disagree with at suggestion. The issue that had arisen was dealt with in a scrupulously fair and measured way. Yes, the defence had been taken somewhat by surprise, but nothing had been suppressed or withheld by the prosecution. The issue would have been discovered if the original exhibits had been inspected by the defence legal team, but they were not. The truth emerged during a cross-examination conducted by counsel for the defence. It was simply one of the hazards of cross-examination, namely, that one sometimes, and despite reasonable preparations, gets an answer that one does not expect. If that were all there was to it then the trial judge arguably did not need to go even as far as she did in attempting to address what had occurred.

204. However, it appears to be the case that prosecuting counsel was equally unaware of the controversial detail, but that once it had emerged he seemingly appreciated its import and was quick to capitalise upon it in his speech. It was not wrong, or an ambush, or unfair, to have done so, in circumstances where what was urged upon the jury was based on evidence that they had heard, and which had been elicited, albeit unintentionally, by defence counsel in cross-examination. We reject the suggestion that it is significant that Ms Lindsey did not say in terms that the garda letterhead was grafted on to the other sheet. That was the clear, and indeed only reasonable, inference that could be drawn from what she belatedly disclosed while being cross-examined.

205. In general, the defence are entitled to have notice of the case that the prosecution intends to make, so that in exercise of a defendant's rights under the *audi alteram partem* rule (s)he may engage with that case and defend against it if minded so to do. In the present case the defence were certainly on notice of the overwhelming thrust of the prosecution's case, although it appears that they did not anticipate that this piece of, essentially collateral, evidence would emerge and be used against them as it was. What occurred was simply one of the hazards of the adversarial criminal procedure by means of which trials are conducted in this jurisdiction. We consider that the trial judge's instruction was enough to redress any slight unfairness to the defence resulting from prosecuting counsel's speech.

206. Accordingly, we are also not disposed to uphold this ground of appeal.

Conclusion

207. In circumstances where we have not upheld any of the grounds of complaint relied upon by the appellant, the appeal against conviction is dismissed.