OVERVIEW OF LIABILITY OF 'INFORMATION SOCIETY SERVICE PROVIDERS' / 'INTERMEDIARY SERVICE PROVIDERS' FOR ONLINE DEFAMATORY MATERIAL

By Michael C. O' Connor, Barrister with the kind and extensive assistance and input of
Dr Ronan Kennedy, NUI Galway Law School
27th November 2015

INTRODUCTION

It has come to my attention that the world of online defamation is quite simply light years away from traditional well-worn defamation principles.

For the most part lawyers above a certain age would prefer to ignore not just European imported online defamation codes but indeed the internet as a whole, email, Facebook, LinkedIn, Google, Apple and any other hocus pocus items such as CD's any suchlike that curiously appeared on the landscape like grotesquely unsightly conifers on mountain sides subsequent to the disappearance of Elvis, vinyl, eight track tapes and record players in the closing stages of the last century.

Not alone have the stubborn imported species taken root but they have steadfastly refused to shed their leaves of liability leaving no option to the storm-troopers of litigation but to try and flatten the trees entirely.

Alas, our European masters have planted these imports deep and the ingenuity of Irish Lawyers will be tested in trying overcome the immunity they have been given.

In order to avoid accusations of over dramatisation it is only fair to point out at the outset that the ordinary Joe and Mary Bloggs who post online are not favoured with the same immunity in law. Their helpful late night and often wine fuelled insights on others are as actionable now as they were!

Relevant Directives, Statutes, Statutory Instruments and key case-law: -

- DIRECTIVE 98/48/EC

- DIRECTIVE 99/93/EC
- DIRECTIVE 2000/31/EC
- ELECTRONIC COMMERCE ACT 2000
- S.I. No. 68/2003 - European Communities (Directive 2000/31/EC) Regulations 2003
- McKeogh v Doe 1 & Ors [2012] IEHC 95
- Tansey v Gill [2012] 1 IR 380
- Mulvaney v Betfair [2011] 1 IR 85
- Tamiz v Google [2013] EWCA Civ 68
- Delfi AS v Estonia (Application no. 64569/09)
- Kaschke v Gray [2010] EWHC 690 (QB)
- The E-Commerce Directive

The law on the legal liability of Internet or online service providers for messages and comments posted by their users is the Electronic Commerce Directive (Directive 2000/31/EC). This is transposed into Irish law by the European Communities (Directive 2000/31/EC) Regulations 2003 (SI 68 of 2003). This applies to those providing an 'Information Society service', defined in Directive 98/48/EC as "any service normally provided for remuneration, at a distance, by electronic means and *at the individual request of a recipient of services*", a definition that is broad and it will be argued broad enough to encompass most, if not all, user-supplied content sites.

'Recipient of services' under the directive means 'any natural or legal person who, for professional ends or otherwise, uses an information society service, in particular for the purposes of seeking information or making it accessible.'

It is arguable that someone who uses the service simply to blacken or abuse others is neither seeking information nor making it available rather they are making available malicious and false representations of falsehoods.

When proven to fall within this definition the directive provides very significant exemptions from liability for such intermediary service providers. There is scope for argument however that the many free services not normally provided for remuneration fall outside the directive. There is also scope for argument that there may well be very arguably a great difference between 'information' in its natural and ordinary meaning and malicious or vile defamatory

remarks or comment that are posted to destroy others and are far removed from what might be considered 'information'.

Oxford online dictionary defines information as '*facts provided or learned about something or someone'*. Confusingly and without any definition the Irish regulations then refer to transmission of 'data' at Article 3. Perhaps its intended that 'data' could cover all sorts of abuse and defamatory material but this appears wider than the Directive.

Article 16 of the Regulations exempts online service providers from liability when they act as a 'mere conduit': -

> *"16. (1) An intermediary service provider shall not be liable for information transmitted by him or her in a communication network if: -*
>
> *(a) the information has been provided to him or her by a recipient of a relevant service provided by him or her (being a service consisting of the transmission in a communication network of that information), or*
> *(b) a relevant service provided by him or her consists of the provision of access to a communication network,*
>
> *and, in either case, the following conditions are complied with: -*
>
> *(i) the intermediary service provider did not initiate the transmission,*
> *(ii) the intermediary service provider did not select the receiver of the transmission, and*
> *(iii) the intermediary service provider did not select or modify the information contained in the transmission."*

Article 18 exempts service providers from liability for hosting content: -

> *"18. (1) An intermediary service provider who provides a relevant service consisting of the storage of information provided by a recipient of the service shall not be liable for the information stored at the request of that recipient if: -*

(a) the intermediary service provider does not have actual knowledge of the unlawful activity concerned and, as regards claims for damages, is not aware of facts or circumstances from which that unlawful activity is apparent, or

(b) the intermediary service provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

(2) Paragraph (1) shall not apply where the recipient of the service is acting under the authority or the control of the intermediary service provider referred to in that paragraph.

(3) This Regulation shall not affect the power of any court to make an order against an intermediary service provider requiring the provider not to infringe, or to cease to infringe, any legal rights."

Article 17 also grants immunity for 'caching' with similar conditions/exceptions.

In general terms I detect an effort to present the position of the service provider as akin to the postal service – a kind of 'Don't shoot the messenger' approach. However the postal service don't deliver mail in see through envelopes or entirely without envelopes. The fact is that these service providers are very often facilitating very cowardly malicious attacks on others and so long as they take it down when asked they can walk away scot free. In the case of Facebook at least the users are usually identifiable however with other providers pseudonyms are allowed and there can be considerable difficulty identifying the culprits. The culprits may then be impecunious and would never have had such a spectacular moment in the sun via a newspaper.

These so-called 'safe harbours' apply to various different types of illegal activity, such as the dissemination of obscenity, child pornography, and copyright infringement. In the particular context of defamation, section 27 of the Defamation Act 2009 is also relevant.

It provides: -

"27. - (1) It shall be a defence (to be known as the "defence of innocent publication") to a defamation action for the defendant to prove that: -

(a) he or she was not the author, editor or publisher of the statement to which the action relates,

(b) he or she took reasonable care in relation to its publication, and

(c) he or she did not know, and had no reason to believe, that what he or she did caused or contributed to the publication of a statement that would give rise to a cause of action in defamation.

(2) A person shall not, for the purposes of this section, be considered to be the author, editor or publisher of a statement if: -

(a) in relation to printed material containing the statement, he or she was responsible for the printing, production, distribution or selling only of the printed material,

(b) in relation to a film or sound recording containing the statement, he or she was responsible for the processing, copying, distribution, exhibition or selling only of the film or sound recording,

(c) in relation to any electronic medium on which the statement is recorded or stored, he or she was responsible for the processing, copying, distribution or selling only of the electronic medium or was responsible for the operation or provision only of any equipment, system or service by means of which the statement would be capable of being retrieved, copied, distributed or made available.

(3) The court shall, for the purposes of determining whether a person took reasonable care, or had reason to believe that what he or she did caused or contributed to the publication of a defamatory statement, have regard to: -

(a) the extent of the person's responsibility for the content of the statement or the decision to publish it,

(b) the nature or circumstances of the publication, and

(c) the previous conduct or character of the person."

The English case of *Bunt v Tilley*[1] makes it clear that Internet service providers who simply provide users with a connection to the Internet (in this case America Online, British Telecom, and Tiscali) are not responsible for the actions of their users. This principle in itself is not

[1] [2006] EWHC 407 (QB).

unreasonable but the further immunity granted for posting of written material via a service providers site is a far more dramatic immunity.

In the Irish case of *Mulvaney v Betfair*,[2] the High Court, relying on *Bunt v Tilley*, found that a chatroom provided by the defendant bookmakers was entitled to the benefit of paragraphs 15 and 18 of the 2003 Regulations. Gambling itself including activities under the Betting Act1931, the Gaming and Lotteries Acts 1956-79 and National Lottery Act 1986 are outside scope of regulations [see article 2]. The chat room in this case where the objectionable material was posted concerning a well-known bookmaker was still held by Clarke J to be within the terms of the regulations. This chatroom service was held to fall within the definition of 'relevant service' as it involved the hosting of information provided by a recipient of the service and available to other users of the service. The judgement is a big impediment to those seeking to impose liability on such providers. The tenor of it suggests favourable and wide interpretations of the immunity. It's not apparent how **'**normally provided for remuneration**'** is being interpreted. The word 'normal' itself has always been a wickedly unclear and divisive word and its use in this directive is to the say the least woolly.

The High Court of Northern Ireland in *XY v Facebook*[3] granted an interim injunction against the defendant social media website removing a page from that site which the court found to be "threatening, intimidatory, inflammatory, provocative, reckless and irresponsible" towards the plaintiff. However, this case was a preliminary hearing in a larger action, and the decision makes no mention of the Electronic Commerce Directive.

WHAT, IF ANY, OBLIGATIONS DO SERVICE PROVIDERS HAVE TO MONITOR CONTENT ON THEIR SERVICES?

Article 15 of the Directive (which has not been explicitly transposed into Irish law) makes it clear that there is no general obligation on intermediary service providers to monitor content on their systems: -

> *"Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they*

[2] [2009] IEHC 133.

[3] [2012] NIQB 96.

transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity."

The European Court of Justice has strongly supported this article in two cases involving attempts by a Belgian association of authors, composers and publishers to require Internet service providers to monitor all transmissions on their network in order to detect copyright infringement.[4] However, the High Court of England and Wales has granted orders against Internet service providers requiring that access to particular websites be blocked on the grounds that they facilitated copyright infringement,[5] distinguishing between a general order against all transmissions across a network and a specific, precise, and not excessively expensive measure.[6]

It is also important to note the recent European Court of Human Rights decision in *Delfi v Estonia* in which the Court considered: -

"... that a large news portal's obligation to take effective measures to limit the dissemination of hate speech and speech inciting violence – the issue in the present case – can by no means be equated to "private censorship". While acknowledging the "important role" played by the Internet "in enhancing the public's access to news and facilitating the dissemination of information in general" ..., the Court reiterates that it is also mindful of the risk of harm posed by content and communications on the Internet ...[7]

While article 15 does not permit Member States to impose any general obligation to monitor, many intermediary service providers do choose to monitor activity on their systems in order to ensure that their online communities develop as they envisage or to guard against unsolicited commercial messages (commonly known as 'spam'). If a provider does choose to monitor, the risk of losing immunity is arises as it is much more difficult to argue that one does not have actual knowledge or is not aware of facts or circumstances on which the illegal activity is apparent. Therefore, the more that the service provider monitors or edits content on

---

[4] C-70/10 Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM); Case C-360/10 Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV.

[5] Twentieth Century Fox v BT [2011] EWHC 1981 (Ch); Dramatico Entertainment Limited v British Sky Broadcasting Limited [2012] EWHC 1152 (Ch).

[6] [2012] EWHC 1152 (Ch) [177].

[7] Case no. 64569/09 *Delfi v Estonia* [157].

its systems, the more likely it is to be held liable for any defamatory or otherwise illegal posting.

KEY QUESTIONS TO CONSIDER

1. Who should I sue?

2. Is it enough to sue the service provider such as Facebook/boards/blogger/google etc.?

3. Is the target an intermediary service provider under the European Communities (Directive 2000/31/EC) Regulations 2003?

4. What, if any, obligations does the intermediary/ information society service provider have to monitor content on their services?

5. Did the intermediary/ISSP have actual knowledge or facts and circumstances from which the alleged illegal activity became apparent?

6. Did the intermediary/ISSP act expeditiously to remove or disable access to the alleged illegal information?

7. Can I identify the person who posted the comment?

8. How do I discover the identity of the person who posts the comment?

9. Can I join the person who posts the comment later? – NB: - Statute of Limitations is only a year extendable to maximum of two years with leave of the Court.

10. If the blogger isn't a mark, do I have any remedy?

11. Can I at least get an injunction?

12. If I can't get damages can I seek a correction order and costs?

13. What constitutes acting expeditiously to remove or disable access to the alleged illegal information?

The English case of *Tamiz v Google*[8] clarifies that service providers which allow users to post content for others to view may, depending on the circumstances, become "publishers" and thus liable in defamation for those posts once they are notified of them. The case involved a claim for damages against Google for comments that appeared in response to a news story on the "London Muslim" blog (which was hosted on Google Blogger service). There was some delay in the removal of the news story and associated comments. The Court of Appeal for England and Wales differentiated between Google's liabilities before and after it was notified of the plaintiff's complaints regarding the comments.[9] The Court relied on the reasoning of the High Court in the similar case of *Davison and Habeeb*[10] that at some point after the intermediary service provider was notified of the comments complained of, it lost its immunity.

The position post-notification was less clear to the Court of Appeal. Relying on the case of *Byrne v Deane*,[11] which concerned an alleged defamatory note posted on the wall of a golf club (which had a rule prohibiting such posting without the consent of the secretary), and where the club was found liable for allowing the posting to remain, the court held that Google could be found liable for the comments once notified of them: -

> *"33. .... The provision of a platform for the blogs is equivalent to the provision of a notice board; and Google Inc. goes further than this by providing tools to help a blogger design the layout of his part of the notice board and by providing a service that enables a blogger to display advertisements alongside the notices on his part of the notice board. Most importantly, it makes the notice board available to bloggers on terms of its own choice and it can readily remove or block access to any notice that does not comply with those terms.*
>
> *34. Those features bring the case in my view within the scope of the reasoning in Byrne v Deane. Thus, if Google Inc. allows defamatory material to remain on a Blogger blog after it has been notified of the presence of that material, it might be*

---

[8] [2013] EWCA Civ 68.

[9] [2013] EWCA Civ 68 [35].

[10] [2011] EWHC 3031 (QB) [46].

[11] [1937] 1 KB 818.

inferred to have associated itself with, or to have made itself responsible for, the continued presence of that material on the blog and thereby to have become a publisher of the material. Mr White QC submitted that the vast difference in scale between the Blogger set-up and the small club-room in Byrne v Deane makes such an inference unrealistic and that nobody would view a comment on a blog as something with which Google Inc. had associated itself or for which it had made itself responsible by taking no action to remove it after notification of a complaint. Those are certainly matters for argument but they are not decisive in Google Inc.'s favour at this stage of proceedings, where we are concerned only with whether the appellant has an arguable case against it as a publisher of the comments in issue."[12]

In light of the *Godfrey v Demon Internet* case,[13] where an Internet service provider was unable to plead the defence of innocent dissemination because they had not acted in response to a complaint from the plaintiff, there remains uncertainty about what constitutes acting "expeditiously to remove or to disable access to the information" complained of.

Not to be underestimated or sipped over tucked away neatly is Article 15.

Article 15 – scene setting or blanket immunity?

"15. A provision of Regulation 16, 17 or 18 providing that a relevant service provider shall not be liable for a particular act shall be construed as a provision to the effect that the provider shall not —

(a) be liable in damages or, unless otherwise provided, be liable to be the subject of an order providing for any other form of relief, for infringing, by reason of that act, the legal rights of

[12] [2013] EWCA Civ 68 [33]–[34].

[13] [2001] 1 BQ 201.

any natural or legal person or, by reason of that act, for breaching any duty, or

(b) be liable to be subject to any proceedings (whether civil or criminal) by reason of that act constituting a contravention of any enactment or an infringement of any rule of law."

SOME CONCLUSIONS

1. The natural instinct to go after what often looks like the obvious 'publisher' must be resisted and the situation carefully weighed up;

2. Self-help methods of finding out who the posters/bloggers are should be explored at the outset. This might be simple on Facebook or LinkedIn etc. It can be a lot harder with sites that use pseudonyms. Nevertheless a good reputable investigator may well find out the identities faster and cheaper than discovery. When the history of such postings are closely examined one will often find out quite a lot about the occupation, interests, location of the subject. If time is devoted the identities may well become known.

3. Obviously a letter seeking the identities should be written to the provider. That letter should also encompass a full data protection request under the Data Protection Acts 1988-2003. The appropriate fee should be enclosed.

4. It must be considered whether the provider has

5. Actual knowledge of the material and whether the facts and circumstances can help establish this;

6. Whether the site has been moderated/controlled/edited – the more of this can be shown the better the chance of a successful suit;

7. Be aware that somewhat strangely the less they interfere and allow the 'notice-board' to its own devices, the harder it is for the plaintiff to win;

8. It's important to write as soon as possible demanding that they remove the material and if they drag their heels in removing it there is a much better chance of success. It's possible that even a delay of several days in removing the material could be found to be not acting expeditiously and certainly if it goes into weeks there is a likelihood of winning against the provider ;

9. The particular task, service or role the provider is engaged in must be considered. There may be an element of the three main labels 'mere conduit', 'caching' and 'hosting' becoming outdated terms as time moves on and bear in mind that these regulations were written in 2003 based on a Directive from 2000.

10. It also has to be borne in mind that by taking on the provider it is going to be an uphill battle against an opponent who will most likely have ample resources.

11. Injunctions to force the taking down of defamatory or abusive material and to prevent it from being re-posted are still available and the best example is the case of McKeogh v. Doe & Others. In fact Peart J in that case relied on the fact that damages are so difficult to get as a reason to conclude damages were not an adequate remedy, hence the need for an injunction.

12. Counsel advising on proofs may well need to consider not discovery (inter party & non-party) but also whether technical and even legal expert witnesses may be required. The area is not at all straightforward and in a difficult case maximum advantage will have to be taken of all weaknesses in the immunities offered.

13. Finally..... as they used to say on *Hill Street Blues,* 'Be Careful out there!!'

MICHAEL C. O' CONNOR B.A, LL.B, LL.M
BARRISTER AT LAW