Presentation to the Law Reform Commission Public Seminar

on

Cyber Crime affecting personal safety, privacy, and reputation, including cyber-bullying

FERGAL CREHAN BL

(*A version of this paper, written with Dr. TJ McIntyre of the Sutherland School of Law, University College Dublin, was submitted by Digital Rights Ireland to the Law Reform Commission in response to its Issues Paper on Cyber-crime Affecting Personal Safety, Privacy and Reputation Including Cyber-bullying.*)

Social media differs from traditional media, with their one-to-many "broadcast" structure, in that it has a 'many-to-many' model, with each member of the audience being a potential outlet themselves. The Internet is not, as some apparently believe an unregulated 'Wild West', as acknowledged by the issues paper. We are in the fourth decade of the Internet's existence. However, in some respects, in Ireland at least, the Internet only broke through to the cultural mainstream since the advent of the smartphone. What might be termed "the Irish Internet community" is to a large extent made of "digital natives", people who have learned appropriate online behaviour over many years' immersion in the norms of the community. At the same time, the law has kept reasonably abreast. We submit that in the areas of bullying and hate speech, two offences exist which are tailor-made, without any amendment, for use in respect of online communication. However, many hundreds of thousands of newer users of the Internet, less attuned to these norms, have flooded online in recent years, leading to an erroneous belief that "anything goes" online.

We submit that this perception has twin dangers. It lulls Internet users into behaving in ways they would not dream of behaving in daily life. It also gives legislators and even enforcers the mistaken impression that no laws exist to deal with such behaviour. However, legislation without enforcement can have little effect. While regard must be had to the right to free speech - including the right to be offensive or even obnoxious – consideration should be given to more frequent prosecution of certain of these existing offences.

1(a):Do you consider that section 10 of the Non-Fatal Offences Against the Person Act 1997 should be amended to include a specific reference to harassment by cyber means?

Section 10 of the Non Fatal Offences Against the Person Act, 1997, provides for the offence of Harassment. Any person who, "without lawful authority or reasonable excuse, by ***any*** (emphasis added) 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". Elsewhere, the section provides for punishment of up to seven years imprisonment, and allows for a court to order, either in addition to, or as an alternative to a conviction, that a person shall not, for such period as the court may specify, communicate by any means, or come within a specified distance of a person's home or workplace. The section, though drafted long before the internet became a part of most people's daily lives, is perfectly suited to the kind of circumstances which prevail in cyberbullying cases. Indeed, it has been used previously in cases where the harassment was entirely via email, and featured no physical element. We submit that the act as it currently stands is more than adequate to online offences. It is merely the enforcement of the section which has been inadequate. We have heard from victims of online harassment who have reported the

matter to the Gardaí and been told that there is simply nothing that can be done in respect of online harassment. This is simply not so, and should be clarified, though it is accepted that investigation of online harassment is time-intensive, particularly where there is a significant geographical distance between the victim and the perpetrator.

In many cases victims will gain more comfort from a restraining order under Section 10(3) than from a conviction. It is a weakness of Section 10 that it does not allow a victim to seek such an order on her own behalf, rather requiring a Garda prosecution in order to bring the matter before a court. **A mechanism should be provided allowing for a victim to make such an application. Given that no victim should be placed at a financial disadvantage as a result of vindicating her rights, we submit that the appropriate means for such an application should be via an application to the civil courts, where an order for costs may be made against the perpetrator of the harassment. it is noted (and will further considered below) that harassment is a statutory tort in the United Kingdom.**

In respect of the online bullying of children and teenagers, we note that such "Cyberbullying" is already illegal. Further, in the much publicised Erin Gallagher case, online bullying was only a part of a range of bullying behaviours directed at Erin Gallagher including, according to press reports, physical assaults on her way home from school[1]. All of this behaviour was illegal but apparently continued notwithstanding this. We note the report of the *Oireachtas* Joint Committee on Transport and Communications, which states:

> *"While the Committee is aware of cases where victims of cyberbullying have taken their own lives, it is worth noting North American research which found that cyberbullying is rarely the sole or main cause of death by suicide."*[2]

We also note that the Anti-Bullying Working Group, in its recent report to the Minister for Education and Skills, made the following recommendation:

> *"at this time, the focus should be on securing implementation of existing legislative requirements across the system rather than seeking to introduce new legislation."*[3]

We endorse this approach. However we warn against any assumption that the criminal law offers an easy solution to the problem of bullying. Prosecution of children as criminals will only rarely be a proportional response to bullying. American Author Emily Bazelon, in her study "Sticks and Stones" has found that prosecutions under the criminal law are rarely effective in countering a culture of bullying, noting that, where children can be simultaneously bullies and bullied, the threat of prosecution can be easily misused as a tool of bullying rather than a remedy for it[4].

1(b):Do you consider that section 10 of the Non-Fatal Offences Against the Person Act 1997 should be amended to include indirect forms of harassment, including persistent posting online of harmful private and intimate material in breach of a victim's privacy?

Section 10 of the Non-Fatal Offences Against the Person Act 1997 requires, to make out the offence of harassment, that a person "harasses another by persistently following, watching, pestering,

1 "Family devastated after tragic Erin (13) takes own life after vicious online bullying", Irish Independent, 29th October, 2012

2 Houses of the Oireachtas Joint Committee on Transport and Communications, Report Addressing the Growth of Social Media and tackling Cyberbullying, July 2013, Ch. 1 , pg. 8

3 Department of Education and Skills, Action Plan On Bullying - Report of the Anti-Bullying Working Group to the Minister for Education and Skills, January 2013, Pg. 63.

4 Bazelon, Emily. *Sticks and Stones: Defeating the Culture of Bullying and Rediscovering the Power of Character and Empathy*. New York: Random House, 2013.

besetting or communicating with him or her". In addition, the offence requires serious interference with the other's peace and privacy, or alarm, distress or harm. Though mindful that this definition does not explicitly provide for indirect communication, as when material is posted in the name of another, we submit that any amendment of section 10 should respect the vital distinction between speech *about* another person and communications made *to* that person. Regular investigative reporting on the affairs of a public figure could be seen as communications causing alarm, distress or even harm. **We submit that the no elision should be made between the intimate communication inherent in the offence of harassment as currently defined, and more public communications, to which certain freedom of speech considerations must apply. In respect of the posting of the harmful private and intimate material in breach of a victim's privacy, We submit that certain other legislative approaches, outlined elsewhere in this submission, are more appropriate.**

1(c):Do you consider that section 10 of the Non-Fatal Offences Against the Person Act 1997 should be amended to provide expressly that it should have extra-territorial effect, provided that either the victim or the perpetrator is based within the State?

In the 1922 debates on the draft Constitution of the Irish Free State, Darrell Figgis' proposal to have universal jurisdiction over Free State citizens was rejected by Kevin O'Higgins, who said

> *"It seems to me that on the question of jurisdiction you come up against this— that if we had set this down in our Constitution that the laws of the Free State were binding on Irish citizens all over the earth, and that Irish citizens in Canada and Australia and America on anywhere else, refused quite to take that view, you come back always to the point as to whether the Government of the country in which he may happen to be accepts that view, and inasmuch as there may be no such agreement, the whole thing is reduced to futility. Are you going, as the President asked, to extradite a man because he refused to obey your vaccination laws at the end of the earth? And is the Government of that particular country going to fall in with your views and assist you to enforce your law in their territory? That is what it comes to. And to set down here in our Constitution a principle of that kind, with no guarantee whatever that it will be honoured or accepted by any single country on the face of the earth is simply inviting ridicule"*[5]

Notwithstanding that *Bunreacht na hÉireann* sets out a much more limited principle of extra-territorial effect, and that the world is perhaps a smaller place now than in 1922, **We submit that no new law in this area should be given extra-territorial effect.**

Without wishing to diminish the harm done by the offences considered in the issues paper, we note that most of them will be tried as summary offences, and submits that extradition is inappropriate for such offences. In the absence of same, or of a provision for trial *in absentia* (which itself would, aside from more principled human rights objections, be meaningless without the ability to actually impose sanctions), there does not appear to be any meaningful purpose to any such extra-territorial effect.

We make this observation in addition to noting the concerns raised in the issues paper regarding speech which might constitute an offence under Irish law but which may be regarded as the permissible exercise of free speech in another jurisdiction.

5 Dáil debates 19 October 1922 Vol.1 No.24 p.4 cc.1742–48

2(a): Do you consider that there should be an offence introduced that would criminalise once-off serious interferences with another person's privacy where carried out through cyber technology?

We submit that while certain additional civil remedies may be required, no further criminalisation of online behaviour is necessary in this area.

As a general rule, the placing of personal information about a person online without their consent will be a breach of the Data Protection Act (DPA). This includes the posting, without consent, of photographs or of video recordings.

The recent unfortunate case where video was posted online of a young girl being indiscreet in a Temple Bar fast food outlet, was clearly covered by the DPA. Unfortunately, the video went "viral", attracting much crude and misogynistic comment[6]. Even those who referred to the video only in order to denounce the breach of privacy played a part in bringing it to a larger audience, and thus inadvertently exacerbated the breach of privacy. Had the girl or her parents been better advised, they might have been able to discreetly have the video removed from Youtube by relying on her rights under the Data Protection Act. Unfortunately, Data Protection, a massively important protection for the modern citizen's privacy, is not widely understood. This must be to a large degree attributed to a historic lack of funding for the Data Protection Commission. The recent rise in funding may help to ensure that privacy rights can be properly and promptly vindicated by the average citizen as well as by the celebrity.

Section 5 of the Non Fatal Offences Against the Person Act provides for an offence of "Threats to kill or cause serious harm". There is nothing in the section to preclude its use in relation to online communications. However, we would caution against over-zealous application of the section, bearing in mind the many colloquial uses of language which, on an objective reading, might appear threatening. The offence requires that the threat is made "intending the other to believe it will be carried out". In this respect, section 5 is superior to the English offence of "Improper use of public electronic communications network", which includes no provision as to the seriousness or believability of a threat. This absence lead to R v Chambers[7], the notorious "Twitter Joke Trial" where a light-hearted tweet caused Mr. Paul Chambers to be convicted under S107(1) of the Communications Act, 2003, requiring him to take his case to the Court of Appeal before he, and common sense, finally prevailed. The *Chambers* case should stand as a warning that absent the element of intention, prosecutions should not be brought.

We note with some concern the recent proposals to broaden the scope of S.13 (as amended) of the Post Office Amendment Act 1951. This section provides that

> "Any person who—
> (a) sends by telephone any message that is grossly offensive, or is indecent, obscene or menacing, or
> (b) for the purpose of causing annoyance, inconvenience, or needless anxiety to another person—
> (i) sends by telephone any message that the sender knows to be false, or
> (ii) persistently makes telephone calls to another person without reasonable cause,
> commits an offence."

It has been proposed that this offence be amended to include all forms of electronic communications. S.13 has existed in its current form since 2007, and it excluded internet

6 "KPMG asks staff to warn them of 'inappropriate coverage' of firm on net", The Journal.ie, 23rd January, 2013

7 [2008] EWCA Crim 2467

communications for very specific reasons. Telephone messages are direct person-to-person communications. A menacing phone call therefore is a very intimate form of harassment. A tweet, Facebook posting or blog post, being viewable by a far larger number of persons, lacks this personal intimacy (emails and twitter "replies" and "direct messages" are already covered by the offence of harassment). Broadening the scope of this offence in the manner described in media reports would create potential criminal liability for any person placing any material on the internet. If would, for example, make it a criminal offence to make any statement online, knowing it to be false. Further, it would make everything on the internet, including the entire output of RTÉ, subject to an offensiveness test. It would also criminalise any form of political art, which often is made with the explicit intention of causing offence, or at least annoyance. These examples are only three amongst a potentially infinite number of absurdities that would be caused by such an amendment of the act. We note that the Report of the Internet Content Governance Advisory Group[8], while recommending the amendment of the 1951 Act, also states

> *"Due consideration should be given in the wording of any such legislation to address the concern put forward by Digital Rights Ireland that amending the Act would place an impossible burden on internet providers by making all online content subject to an offensiveness test."*

We are far from certain that this concern can be met whilst amending the 1951 Act in the manner contemplated. Certainly, any such amendment would be required to be drafted in such a manner that it applied to communications directed specifically to an individual person rather than simply relating to that person but published to the world at large. In the absence of such a limitation, any such offence would constitute a speech crime rather than a crime against the person. In light of Ireland's free speech obligations under national, European Union and International law, such a distinction is crucial. Quite apart from the practical difficulties presented, it is our view that the criminalisation of offensiveness (as opposed to the harassment or bullying of specific persons) is, even if a satisfactorily stable definition of "grossly offensive" were possible, incompatible with those obligations. Accordingly, we do not believe that the appropriate means of protecting individuals from once-off invasions of their privacy is the amendment of or the institution of any similar offensiveness-based provision.

We submit that the invasion of privacy is an infringement of a personal right, and that accordingly any effective remedy ought to be available to the citizen herself, independently of the ability or willingness of the *Garda Síochána* to bring a prosecution. We detail our proposals for civil remedies below.

2(b): If such an offence were to be introduced, do you consider that it should have extra-territorial effect?

We reiterate our position on extra-territorial effect of criminal laws as outlined above in its answer to question 1(c) above.

2(c): Do you consider that any further reforms to the criminal law are needed to target harmful cyber behaviour affecting personal safety, privacy and reputation?

We note with approval the principal conclusion of the UK House of Lords Communications Committee's report on Social Media and Criminal Offences:

8 Department of Communications, Energy and Natural Resources, Internet Content Governance Advisory Group report, May 2014, Pg. 45

"Our overall conclusion is that the criminal law in this area, almost entirely enacted before the invention of social media, is generally appropriate for the prosecution of offences committed using the social media."[9]

We reiterate our position that where there are deficiencies in the criminal regulation of harmful online behaviour, they are in the area of enforcement rather than in the legislative regime. The most appropriate response is the provision of greater funding and training for Gardaí in this area.

Q3:Do you consider that the Prohibition of Incitement to Hatred Act 1989 and the Criminal Justice (Public Order) Act 1994 adequately address hate speech activity disseminated through cyber technology and social media?

We believe that hate speech is adequately addressed by existing law, though deficiencies exist in the area of enforcement. Even so, we submit that a distinction must be made between the legitimate use of social media as a political organising tool and the incitement of violence, for example against minority groups

We believe that the Prohibition of Incitement to Hatred Act, 1989 is technology-neutral, and as such is entirely adequate to address hate speech online and off. It provides, *inter alia*, for an offence of "Preparation and possession of material likely to stir up hatred". This offence is strictly limited to hatred on grounds of race, colour, nationality, religion, ethnic or national origins, membership of the travelling community or sexual orientation. The section was relied upon in a prosecution in Killarney District Court, when a 27 year old Kerry man published materials on a Facebook page that were both threatening and abusive to the Traveller community[10]. The case was dismissed; on the stated grounds that there was a reasonable doubt that there was an intent to incite hatred. This finding was somewhat surprising, as the section provides that an offence is committed where the stirring up of hatred is intended, or is likely. The 1989 act is a technology neutral one, as appropriate to online expressions of hatred as it is to those occurring offline. Any weakness in the decision in the Kerry Facebook case does not, in our view stem from the inadequacy of the legislation. That decision, whatever the reasons for it, is an unfortunate one, in that it is likely to have a chilling effect on any further prosecutions.

It should be noted that Section 6 of the Criminal Justice (Public Order) Act 1994 does not apply to the online environment which is not a "public place" as defined by s.3 of that Act, and indeed the overall scheme of the Act makes it clear that it is intended to apply to physical spaces only. Public order offences are predicated on the basis that immediate physical confrontation and direct violence may result from certain behaviour in public places. This rationale has no application to communications online and it is unhelpful to conflate the two situations. Further, the online viewer has chosen to view a particular web site, and at all times has the option to cease viewing it. The person on the street may be involuntarily exposed to the offensive words or actions, and may find it difficult to avoid.

Q4 :Do you consider that the current penalties under the offences which can apply to cyber-harassment and related behaviour are appropriate?

We believe that the penalties applying to harassment offences are suitable to the gravity of the offence, and allow adequate latitude to courts to correctly gauge the seriousness of the specific

9 House of Lords Communications Committee, First Report – Social Media and Criminal Offences, 22nd July, 2014, Ch. 1, Paragraph 5.

10 "Facebook Traveller rant was a 'once-off'", Irish Independent, 1st October, 2011

offences before them. We believe that there is no public concern at the inadequacy of these remedies, but rather at the infrequency of prosecutions. We submit that notwithstanding this, the criminal law may not be the best or the sole means by which this problem can be remedied. Again, we submit that civil remedies may be a more practical solution in many cases.

5(a): Do you consider that in addition to section 10(5) of the 1997 Act there should be a separate statutory procedure, to provide for civil remedies for cyber-harassment and serious interferences with an individual's privacy, without the need to institute a criminal prosecution?

Cyber-harassment

We note that the United Kingdom has, since 1997, a Protection from Harassment Act, which operates a hybrid criminal-civil system. This Act provides for a claim in civil proceedings (creating a statutory tort) by anyone who is or who may be a victim of conduct falling within its definition of the offence. It provides for damages for anxiety caused by the harassment and any financial loss it causes, as well as providing for an injunction to restrain the defendant from conduct amounting to harassment. Where any person against whom an injunction has been granted under this section does "without reasonable excuse" anything prohibited by that injunction, section 3(6) of the Act makes that person guilty of an offence.

We submit that, notwithstanding certain flaws in the UK Act's definition of harassment, consideration should be given to adopting its hybrid criminal-civil system in this jurisdiction. We submit that the main deficiency in the current Irish law of harassment is not in its applicability to online behaviour, but in the rarity of prosecutions**. We submit that the creation of a statutory tort, with damages for distress, would provide a real deterrent against harassment and place an effective remedy directly in the hands of the victim, while still allowing for criminal sanction in the most egregious cases.**

Interferences with Privacy

We note that in the vast majority of cases, online breaches of privacy involve the distribution online of the personal data, usually imagery, of the victim. As such, these actions are an infringement of the right to Data Protection, as provided for under the EU Charter of Fundamental Rights, Bunreacht na hÉireann and the Data Protection Acts 1988-2003 (themselves an implementation of Directive 95/46 EC).

The remedies provided under data protection law are, we submit, ready-made for dealing with such offences as "revenge porn". Lilian Edwards, professor of internet law at the University of Strathclyde, Glasgow, and Specialist Adviser to the Lords Select Committee on Communications report on social media and criminal law (cited above), has written

> *"A good remedy for the UK thus involves two steps : mandatory take down of images posted without consent from hosting sites in the UK, and, if take down is not obtainable because the host site is in the US and hiding behind a liability shield, a right to removal of the link from Google's memory so a search on a name will not bring up as first result shocking pictures posted and hosted without consent.*
>
> *Many press reports have responded negatively to the recent Google Spain European Court of Justice case, which held that a person has the right to have a link relating to their name*

which is inaccurate, misleading or distressing removed from the search engine – the so-called "right to be forgotten".

Whether you view this as a vindication of basic rights to control our own personal data online, or a worrying trend for the public record online, it is an undoubted godsend to revenge porn victims. Google is the search engine of choice for around 90% of European users – if a link vanishes from their index, the content essentially ceases to exist."[11]

We submit that the basis for such a remedy already exists within the Data Protection Acts. Section 6 provides for the Right of Rectification or Erasure, requiring data controllers, within 40 days, to rectify or erase any data being processed by them in contravention of the act. This would include images posted on the internet without the consent of the person portrayed. In addition, Section 6A provides for Right to Object to processing likely to cause distress. This requires data controllers to cease within 20 days processing of data likely to cause substantial damage or distress to the data subject or to another person, and, where that damage or distress is or would be unwarranted. This too covers the posting online of images without the consent of the person portrayed.

We submit that consideration be given to shortening the time limits for rectification and the cessation of processing likely to cause distress, to reflect the technological reality of social media. By the time a right of erasure has been upheld, the material in question will often have gone viral.

We submit that where a data controller does not comply within the time limits with a request to rectify or erase under Section 6, or to cease processing under Section 6A, that a civil remedy should lie in the courts against that data controller. We submit that the existence of such a remedy will provide an incentive to the major web services, many of which are based in Ireland, to comply with such requests with the same alacrity with which they comply with take-down requests made pursuant to ownership in copyrighted material.

Such a tortious right of action is already provided for under Section 7 of the Data Protection Acts. However, this tort is actionable only where loss can be shown as a consequence of the breach of Data Protection Rights. Accordingly, no remedy is available in respect of the great distress caused to persons who find their intimate data shared with the world at large through the failure by data services to properly secure their data (as, for example in the recent hack where intimate images of a large number of celebrities were obtained from cloud services). We note that an action in Breach of Confidence already exists, but there is no clarity as to whether it is a reliable remedy in such cases.

We submit that the right of action already provided for under Section 7 of the Data Protection Acts should be made actionable *per se*, or in the alternative that it be actionable in respect of distress, upset and inconvenience.We note, in this regard, the recent UK decision of Vidal-Hall v Google[12] which established the existence of a tort of misuse of private information.

5(b): Do you consider that any further reform of civil proceedings, over and above those in the 2014 Report of the Internet Content Governance Advisory Group, are required?

Defamation

According to the Defamation Act, 2009, and to settled case law, a defamatory statement means "a statement that tends to injure a person's reputation in the eyes of reasonable members of society".

11 "Revenge porn: why the right to be forgotten is the right remedy", The Guardian, 29th July, 2014

12 [2014] EWHC 13 (QB)

However, courts have long taken the view that crude and vulgar abuse is not capable of being defamatory. This type of abuse is all too often seen on-line. Such abuse may, however, constitute a criminal offence.

In principle, defamation online is no different from in any other medium. However, a recent line of English cases has placed some restrictions upon the application of the UK Defamation Act to online publication, and it is not unlikely that Irish courts will follow similar lines to those described below.

Extent of Publication

In order to prove defamation occurred, it has always been necessary to show that publication actually occurred. A copy of a newspaper or a recording of a broadcast will tend to be good evidence of publication, and a court will infer the extent of publication from the scope or distribution of the publisher or broadcaster. However, this is not necessarily enough in the case of online publishing, since it does not follow that because something was placed on the internet, it was necessarily read by a large number of people or indeed anyone at all. Accordingly, a court will not simply assume that publication occurred, and will require evidence that the offending material was seen or heard.

In *Tamiz v Google*[13], the English Court of Appeal held that

> *"it is highly improbable that any significant number of readers will have accessed the comments after that time and prior to removal of the entire blog. It follows, as the judge clearly had in mind, that any damage to the appellant's reputation arising out of continued publication of the comments during that period will have been trivial; and in those circumstances the judge was right to consider that "the game would not be worth the candle"*

Though the reasoning in this case and its antecedents has not been explicitly approved in an Irish judgement, it has persuasive authority. In any case, where the defendant in such a case is a private individual, perhaps not even an adult, simple cost considerations will discourage many plaintiffs. Further, public figures may wish to reflect on which is a greater affront to their dignity, the words of an ill-informed teenager, or the publicity garnered by pursuing that teenager through the courts.

We submit that the extent of publication has always been a consideration in defamation cases in this jurisdiction, and that it should be so *a fortiori* in cases of online publication, where publication may not exceed a handful of readers, unless wider attention be drawn to the statement by the Plaintiff herself.

Publisher's Liability in Defamation

The Defamation Act provides for liability for defamatory statements on the part of author, editors and publishers. Prior to the emergence of social media, these categories were easily defined. Online, though an author is easily defined, there has been some dispute as to what constitutes an editor or publisher. The question is further affected by the EU "E-Commerce Directive[14]", as transposed into Irish law. That directive allows certain persons to plead that they are a "mere conduit" for certain information, and thereby not liable, should the information give rise to civil or criminal liability, just as telephone companies are not liable for the content of phone calls. Certain other providers of services are in a less secure position. Facebook, Twitter, and domestic sites like Boards.ie have long sought to avail of the mere conduit defence, on the basis that they are merely providing a platform

13 [2013] EWCA Civ 68

14 Directive 2000/31/EC on electronic commerce

for user-generated speech. However, by taking a role in moderating and monitoring content, they may be taking on the role of editors or publishers. The usual practice has been to operate a "notice and take down" policy, removing offending content upon receipt of a complaint. The above-cited *Tamiz* case offers some backing for the policy, the Court of Appeal having held that Blogger, a blogging platform owned by Google, could be held liable for content on their platform where Google failed to act promptly on the receipt of a complaint. Though Google ultimately avoided liability on the grounds cited above, the Court held that Google could be held liable as publishers if they failed to take prompt action once the existence of the offending publication became known to them. Action taken five weeks after receipt of a complaint was held not to be prompt.

The trend seems to be for Notice and Take Down to become standard practice. Indeed, we submit that the balance is problematic from a Freedom of Speech point of view. It places companies like Google (or far smaller companies like Boards.ie) in the position of having to decide on the validity of complaints. A defamation trial can last days. In order to avoid liability, administrators for sites like Boards.ie, without any legal expertise, are required to make a snap judgement on whether a statement is defamatory. Inevitably, they err on the side of caution, and perfectly legal statements will be deleted under the mere threat of legal action. This is an example of what the European Court of Human Rights has called a "chilling effect". Further, it is an open invitation for those who are the subject of criticism to silence critical comment without ever having to prove their case.

We submit that as a result of this natural balance in favour of the subject of criticism, the current provisions regulating moderation of social media platforms already offer more than adequate protection to those who consider that they have been wronged.

Anonymity

As a preliminary point, we wish to state that anonymity serves a socially useful purpose. Throughout history, authors have found it necessary to adopt alternative names for their public statements. In 2010, anonymous blogging alerted us to problems within the Irish Red Cross which might never have come to light had the blogger not been able write under a pseudonym. Ultimately, the anonymous blogger was unmasked by the Red Cross, who dismissed him from his employment with them. Indeed, where the current government has recently enacted "whistleblower" protection legislation, any further attack on the right to anonymity would seem to be a retrograde step.

We also note that the UN Special Rapporteur on Freedom of Expression recently called on States:

> *"to ensure that individuals can express themselves anonymously online and to refrain from adopting real-name registration systems. Under certain exceptional situations where States may limit the right to privacy for the purposes of administration of criminal justice or prevention of crime, the Special Rapporteur underscores that such measures must be in compliance with the international human rights framework, with adequate safeguards against abuse. This includes ensuring that any measure to limit the right to privacy is taken on the basis of a specific decision by a State authority expressly empowered by law to do so, and must respect the principles of necessity and proportionality."*[15]

In practice, it is impossible to enforce the use of real names prior to publication online. Even where users provide a plausible real name to social media platforms, the platform cannot know, and has no way of verifying, that the name is in fact the true name of the user.

15 United Nations Human Rights Committee, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, 2011, 22, http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

In 2008, the popular Korean actress Choi Jin-sil, died by suicide, a death tied in the public imagination to rumours about her circulating online. The South Korean government responded by instituting a "real names" policy, which required domestic websites to require all users to provide their real names, as a condition of use of the web service. Users were required to verify their identities by submitting their Resident Registration Numbers (RRNs) when signing up to social media sites. Many major sites (including Youtube) refused to do so, preferring instead to ban all Korean users from publishing on their services.
In addition, the personal information harvested by websites became a treasure trove for identity thieves, leading to data breaches so widespread that the South Korean government believes it will have to issue new Resident Registration Numbers to the entire population, at a cost of billions of dollars.

On August 23, 2012 the Constitutional Court of Korea ruled unanimously that the real-name requirements were unconstitutional. The Court held,

> *"The system does not seem to have been beneficial to the public. Despite the enforcement of the system, the number of illegal or malicious postings online has not decreased. Instead, users moved to foreign websites and the system became discriminatory against domestic operators. It also prevented foreigners who didn't have a resident registration number here from expressing their opinions online"*[16]

We submit that any attempt to enforce use of real names online would be all but impossible to effectively enforce, and that any meaningful enforcement would require an almost Orwellian system where citizens are required to hand over their PPSNs prior to their expression of even the most anodyne views. We note that, since the demise of the South Korean Real Names policy, the only state which now has such a policy in place is the People's Republic of China, frequently criticised by the Irish government for its disregard of human rights, including Freedom of Expression[17]**.**

Norwich Pharmacal Orders

It is widely believed that persons on the Internet are anonymous and untraceable. This is not so. In many cases, real names, or easily understood variations thereof, are used as "handles". In others, the Internet itself provides the tools to identify an individual by context. For example, persons writing under a pseudonym will often link to photos and other details about work and family, making their identity easily discoverable. Where actual anonymity exists, legal remedies are available. A *Norwich Pharmacal* order may be sought from the Courts to unmask anonymous or pseudonymous persons on the Internet. These orders are typically made against hosts of internet platforms, requiring them to disclose IP number from which the abusive comments were made, and then against Internet Service Providers (ISPs), requiring them to identify the subscriber linked to that IP number.

In 2005, the High Court held that "The right to privacy or confidentiality of identity must give way where there is prima facie evidence of wrongdoing. There is such evidence here". In 2012, the High Court made a Norwich Pharmacal type order against a number of proprietors of message boards, at the application of an exploration company which alleged defamation by certain pseudonymous persons. The Court did so having found that there was *prima facie* evidence of wrongdoing, in this case, defamation.

In an English case concerning alleged libel on an Internet bulletin board, the Court of Appeal ruled

16 2010 Hun-Ma 47
17 "President raises human rights issues with Chinese", Irish Independent 10th December, 2014

that it would be disproportionate to grant an order disclosing the identity of the author because the applicant had not established an arguable case of libel. The Court provided guidance on the quality and quantity of the evidence needed to support a Norwich Pharmacal order and ruled that applicants for such orders need to provide the court with a coherent body of evidence which allows for an allegation of wrongdoing to be properly assessed. Later that year, the English High Court refused to grant an order relating to the identity of persons who "may have" engaged in illegal activity, and ruled that "Norwich Pharmacal does not give claimants a general licence to fish for information that will do not more than potentially assist them to identify a claim or a defendant" .

We believe that the Norwich Pharmacal procedure provides a more than adequate remedy for the individual seeking to unmask anonymous persons. We submit that its weakness is in the absence of safeguards to prevent persons being unmasked without due cause. Unlike other jurisdictions such as the United States, Irish law fails to ensure that users are notified of attempts to identify them and given an opportunity to oppose the application. Consequently in most cases Irish users are dependent on the web platform or ISP to notify them of the application and to make a case on their behalf. These companies however, have no commercial incentive to do so.

These issues are also illustrated by *Ryanair v. Johnston*[18]. In that case Smyth J. held that a Norwich Pharmacal application brought by Ryanair to identify pilots who posted to a union run internet forum should be denied where there was no evidence to support the plaintiff's claim and the plaintiff had acted in a manner which was "bullying" and even "tyrannous". Instead, the action (along with a criminal complaint by the plaintiff regarding the internet postings) was found to be part of a wider attempt to intimidate Ryanair pilots who were involved in an industrial dispute. Per Smyth J.:

> *"The pleaded concern and invocation of the statutory duties arising from Safety Health & Welfare at Work Acts 1989-2005 and the regulations and statutory instruments made thereunder, and the Code of Practice detailing procedures for addressing bullying in the workplace was to lend a facade of concern on non-issues in what was essentially a reaction by the Plaintiff against the want of an immediate and unequivocal acceptance of non-negotiable terms and conditions laid down to the Defendant by the Plaintiff referable to retraining. The real as opposed to the putative purpose of any investigation was to break whatever resolve there might have been amongst the captains to seek better terms and, in particular, a very reasonable and justifiable concern over Condition 3(b) and the matter of pensions in particular. In my judgment on the evidence before the Court, there was no warrant for the seeking assistance from An Garda Siochána, this seemed to me to have all the hallmarks of action in terrorem…*
>
> *In real truth this action is part of the ongoing conflict between Union recognition at Ryanair and the company's determination to resist this and I express no view on either party's position. The "sole discovery" action it appears to me forms part of a war of attrition that the captains are to be dissuaded by legal battle from having the temerity to try to achieve their aim if it be such."*

It would have been a grave injustice had the constitutional and statutory rights of these pilots to privacy been taken away in these circumstances. However, the Court was only in a position to make

18 (unreported, Smyth J., 12 July 2006, available at https://www.scribd.com/doc/83471166/Ryanair-v-Johnston)

these findings due to the fact that the Norwich Pharmacal action was brought against a union which was willing to stand up for these rights. Had the action been brought against a commercial provider then it would have been under no obligation to notify the pilots of the attempt to identify them, much less to challenge the action in any way.

In our experience, internet service providers do not generally notify affected users and normally adopt a neither consent nor oppose posture in response to a Norwich Pharmacal action, with the result that the High Court is called upon to make a determination based on the unchallenged evidence of the plaintiff. In the Ryanair case, this would most likely have resulted in an order being made to identify the pilots based on evidence which (when tested) Smyth J. later determined to be variously "baseless and false" and "difficul[t] to believe".

It is therefore deeply undesirable that Norwich Pharmacal orders are granted on what is effectively an *ex parte* basis, particularly where the effect of the order is irreversible.

We submit that the anonymous user should be given an opportunity to make representations to the court before they are stripped of their anonymity. This could best be done by adopting the procedure suggested in *Totalise plc. v The Motley Fool*[19], *i.e.* requiring the ISP to notify the user, and then allowing the user to make written submissions via the ISP. In addition, the user should (if they wish to instruct lawyers) be given the opportunity to be heard on the application, via a mechanism that will preserve their anonymity. It is submitted that some such procedure must be adopted if unwarranted infringements on the right to anonymity are to be avoided.

We also submit that consideration should be given to placing the Norwich Pharmacal procedure on a statutory basis, with a meaningful and rigorous threshold required of applicants. We further submit that in the interests of access to justice, consideration should be given to assigning such applications to the jurisdiction of the Circuit Court.

5(c): Do you consider that complaints of cyber-harassment and other harmful cyber activity affecting personal safety, privacy and reputation should, without prejudice to any criminal proceedings, be considered by a specialist body that would offer non-court, fast yet enforceable remedies?

We submit that questions of cyber-harassment and other harmful cyber activity affecting personal safety, privacy and reputation do not require, for their resolution, any specialist technical expertise. These are offences against the safety, privacy and reputation of the individual, as capable of being carried out online as off. Accordingly, the only appropriate expert body to adjudicate such claims is a court of law.

Further, we dispute the premise that a non-court body could offer remedies any fast than a court, especially where that non-court body's procedures are without prejudice to any criminal proceedings. Where the harmful activity complained of is undertaken maliciously, it is unlikely that it will cease on foot of anything short of an order of the court. Accordingly, pursuing a complaint through a non-court body would serve only to draw out proceedings. Given the viral nature of social media, time is often of the essence. We submit that the institution of criminal or civil proceedings has an immediate chilling effect on the misbehaving party unrivalled by any non-court process. Finally, We submit that if Ireland hopes to make itself a world capital for the data industry, it must

19 [2001] EWCA Civ 1897

show itself to be serious about the rights to Privacy and Data Protection. Accordingly, any and all laws providing for such rights must be rigorously enforceable, using all the tools at the disposal of the litigant, and subject to all the appropriate rules of court. The creation of a non-court body to adjudicate such controversies would be rightly be seen internationally as a relegation of these rights to secondary status.

5(d): Do you consider that further reforms are required to make effective any orders in civil proceedings that would have extra-territorial effect, including in their application to websites located outside the State; and if so do you have any comments on the precise form they should take?

We acknowledge the difficulty in making effective outside of the State certain orders in civil proceedings. However, we submit that these difficulties are not attributable to the lack of extra-territorial effect of any law or rule of court. **We submit that the appropriate means of making such orders enforceable abroad is by way of the negotiation of treaties on a EU or international level.**