International Conference on Law Reform

11 and 12 April 2015

at Royal Society of Edinburgh, Edinburgh, Scotland

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

Finola Flanagan, Commissioner, Law Reform Commission, Ireland

Cyber-technology has transformed communications and our world by allowing us to publish online, instantly, to vast audiences, permanently and in many cases without thought. It has positive aspects in that it allows us to remain connected. At the same time it facilitates cyber-harassment and online abuse. Abusers of the internet often behave in a disinhibited fashion where they do not see the effects of the harm they cause when they publish to global audiences or to circles of "friends". Ireland's problem is that our harassment laws do not catch all abusive conduct in the cyber-world that should be criminalised. It does not catch for example all abusive material published once only and not persistently, or harmful material published about a person and not directly to them. There are few prosecutions for abusive online behaviour and civil remedies are often considered inadequate or ineffective. This is a serious matter and we are aware that bullying online causes much pain and can have devastating consequences which may even lead to suicide if the victim is sufficiently vulnerable.

The project entitled *"Cyber-crime affecting, personal safety, privacy and reputation, including cyber-bullying"* is part of our Fourth Programme of Law Reform adopted in 2014. Apart from looking at the cyber-bullying and privacy issues mentioned in the title, we will look at how the law on hate crime intersects with cyber-crime. We will also look at

jurisdictional questions including extra-territorial jurisdiction, penalties and, most importantly, civil remedies.

The Law Reform Commission is therefore examining the following questions:

Is our current law sufficient for the purpose or adaptable so as to become so? or

Is a dedicated new law required? or

Are both of these approaches required?

We published an Issues Paper on 20 November 2014 seeking responses to fiveissues. This can be seen – and answered – on our website at http://www.lawreform.ie/_fileupload/Issues%20Papers/ip6Cybercrime.pdf

(We will not be addressing cyber-crime in all its forms such as hacking or attacks on cyber systems offences, and fraud conducted on the internet. Nor will we examine issues connected with online child pornography, trafficking or matters such as illegal trade in drugs or arms on the Darknet.)

We decided to examine this matter after wide public consultations. There were many requests asking us to examine issues relating to new technologies and in particular issues of bullying, privacy, voyeurism, stalking and online incitement to hatred and hate crime.

At our conference in Dublin Castle in 2007 the Honorable Justice Michael Kirby, Justice of the High Court of Australia and one-time Chairman of the Australian Law Reform Commission, described what he saw as the fundamentals for success of institutional law reform. In doing so he observed that law reform ought not to be left to the judges as they were too dependent on the chance that the right case would come before them and, if it did, on the further chance that it would come before a judge who was prepared to take the opportunity to make new reforming law. This is especially so in a jurisdiction like Ireland where the pool of cases is small.

He considered that law reform ought not be left exclusively to parliament either because in parliament's eyes a topic might be "too hot" at a particular time (instancing the interface between the laws of the settlers and the laws of the indigenous peoples of the Australian

continent) or “too cold” (instancing an aspect of bankruptcy law – though following the financial crisis in Ireland a Law Reform Commission Report on personal insolvency in 2010 influenced the enactment of a reforming Act in 2012) as well as the possibility of it becoming stuck in the logjam of the lawmaking process. When Geoffrey Palmer (former Prime Minister of New Zealand and former President of the New Zealand Law Commission) delivered the Scarman Lecture in London in March 2015 he expressed frustration at the Executive’s poor performance on the law reform front.

Our project on cyber-bullying is neither too hot nor too cold being a serious social issue needing urgent action with no single solution. Furthermore it has the support of the Executive in the person of a former Minister for Justice and Equality and departmental officials who requested that we address it. In other words for us this programme is, like Goldilocks’ porridge, “just right” and we expect that our recommendations will get the attention of the Executive when we make them and hopefully their support.

At this stage of the project we have not yet reached conclusions and are still information-gathering and consulting. What you hear today are my views as coordinating commissioner of the project. We will be holding a public seminar on 22 April when Sir Michael Tugendhat, the recently retired High Court Media Judge of England and Wales, will deliver the keynote address. We hope if at all possible to deliver our report with recommendations by the year’s end.

These are matters which have already been examined extensively by others at home and abroad in a variety of contexts such as by a parliamentary committee, by the Internet Content Governance and Advisory Group established by our Minister for Communications, Energy and Natural Resources, by the EU in the context of the data protection regime and in relation to child internet safety and by other law commissions such as the New Zealand Law Commission who produced a report in 2012 and by many other bodies throughout the world.

The online world is a new world. We are living in the digital age in which the online world is not just a means or medium of communication but a new environment and, for younger people especially, a real place. This is a place which the inhabitants mean to be free and

open, uncensored, where free speech is central and anonymous if desired. Online anonymity is seen as giving privacy to those who enter this world. Lilian Edwards (Professor of internet law at the University of Strathclyde) advised a House of Lords Committee on social media but disagreed with the Committee's call that social networks require people to register with them using their real names. She said "I think people have a right to speak online about, for example, their politics, their sexuality, their health, their love life, without constantly worrying that at some future point a government/employers/insurers may get access to their true identity." However despite this apparent privacy every online interaction is permanently associated with the maker. Thanks to Edward Snowden we are aware of the extent of mass surveillance of our online activities by states, and Max Schrems seeks to show how social media sites can be complicit. This is so notwithstanding the guarantees protecting personal data and privacy in the EU Charter of Fundamental Rights. That corner of Winston Smith's room where he could huddle out of sight of the telescreen and Big Brother's observation is not available to those who go online.

Whilst many would say that anonymity online allows for privacy and freedom of expression it also allows for cyber-harassment and abuse. It encourages people to behave in a disinhibited fashion because they do not see the effect of what they say.

We all know of virulent abuse doled out online to public figures. An example is the treatment by trolls of Caroline Criado-Perez who innocently, one would have thought, campaigned to have more women depicted on British bank notes. She was subjected to numerous threats, including threats of rape and murder, on Twitter from the day the Bank of England announced that it was intended to put an image of Jane Austin on the £10 note. At one point Criado-Perez was receiving about fifty such threats an hour. Several people were convicted of improper use of a communications network and imprisoned.

It is clear that harmful behaviours online need to be addressed and privacy rights need to be protected. Law as it affects online behaviour needs to be evaluated for adequacy, appropriateness and effectiveness.

Some say that the law for online and offline activity should be the same - that the law should be "technology neutral". For many this is a given and not for argument. However it

is not clear to me that this is correct. To my mind the pertinent questions are whether in fact the law protects rights both online and offline and whether the law achieves a balance, where needed, between various rights and in this context between the right to privacy on the one hand and the right to freedom of expression on the other. In my opinion a special regime for online behaviour may well be required so as to take proper account of its extreme effects which, in general, are not present where the same activity is carried out offline.

We do not want to shoehorn new behaviour into old offences where interpretations are stretched and the law made unclear. For instance it was suggested in the course of our researches that our Criminal Justice (Public Order) Act 1994 sections 6 and 7 which create offences of provoking a breach of the peace "in a public place" might be extended by amendment to apply to the internet because the internet was a "public place". Whilst online conduct which provoked a breach of the peace *on the street* would be capable of being an offence within the section, using this provision to criminalise online conduct causing an *online attack* on an individual or group would introduce a new concept of what was a breach of the peace quite different from what was originally envisaged by the legislators.

The questions for the Law Reform Commission are how to regulate and the extent of regulation. Some recommend limited regulation because the structure of the internet creates major difficulties in identifying the authors and in enforcing remedies, civil or criminal, against them.

Some say cyber-space should be left free and open, with no central regulator and where social networking services have a passive editorial rule as prescribed in the E-Commerce Directive which defines them as "mere conduits" who are not responsible for content if they do not knowingly act to promote harmful or illegal material and act expeditiously to remove any such content once notified by competent authorities.

Others seek extensive regulation.

Whichever approach is taken account must be taken of the fact that law is not the only answer nor is it a comprehensive answer to online wrongdoing. Education, training and

social policy all have essential roles to play. The Law Reform Commission is examining legal solutions and we already have a considerable body of legislation which can be applied to online offences, such as:

- harassment;
- grossly offensive, indecent, obscene, false or persistent telephone or text messages;
- hacking; and
- Data Protection Acts 1988 and 2003.

Harassment

In our Issues Paper we examine the 1997 offence of harassment, prosecutable summarily and on indictment, which comes from pre-internet days and, indeed, from a recommendation in a Law Reform Commission report in 1994.

> "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."

This makes an offence of "communications by any means" which if done once would not necessarily be criminal but which becomes so by virtue of persistence or repetition. The standard is objective such that a reasonable person would have to realise that their conduct would cause harm. There have been approximately six prosecutions in Ireland related to online harassment of which we are aware and all have resulted in pleas of guilty. However there is no specific reference in the section to communications by "cyber means".

The question we ask is whether we should expressly include cyber-communication as a means of communication even though it is accepted that cyber-communications are already covered by the term communication "by any means". A majority but not all of those who responded considered that its express inclusion would increase reporting of cyber-harassment especially in relation to children; that it would bring clarity and mark its seriousness.

As part of this Issue we also address indirect harassment i.e. persistent communications by email, on public websites or on social networking sites such as Facebook to third parties *about* the complainant but *not made directly to* the complainant. These are probably not captured by the harassment offence. By contrast, the English Protection from Harassment Act 1997 is specifically designed to do so. "Revenge porn" is a particularly notorious form of indirect harassment. An example is the mass release in 2014 of intimate photographs hacked from the online account of well known personalities such as Jennifer Lawrence. Whilst the majority of responses to the Issues Paper on this subject agreed that indirect harassment should be expressly included because this type of abuse should be criminalised and not excluded on the basis of a perceived "technicality", nonetheless others who responded (including a social networking site) considered that to include indirect harassment expressly in the offence "would represent a fundamental change in the law of criminal harassment" which currently requires "a direct nexus between the perpetrator and the victim". One social networking site suggested that the effect might be to criminalise off- and online gossip or rumours and that criminal liability might be created for sharing lawful content such as a post on Facebook which detailed the criminal convictions of a paedophile.

The Crown Prosecution Service guidelines and the Scottish guidelines on social media prosecutions recommend that a high degree of care be taken by prosecutors in order to protect freedom of expression especially where there is no breach of a court order, no threats or no individual is targeted.

Once-off serious interferences with another person's privacy

Another issue examined was whether "there should be an offence introduced that would criminalise once-off serious interferences with another person's privacy where carried out through cyber-technology". Our offence of harassment requires persistent conduct and therefore probably does not criminalise a single upload even when it persists over time on the internet and even when it goes viral. A new offence would require an interference with a person's privacy by a single upload provided the communication was sufficiently damaging to the victim even if it was not menacing, abusive, obscene or a hate crime. The communication would have to cause serious damage by publicly shameful or humiliating material being placed on a public website or a social networking site. Two examples to which we refer in our Issues Paper prompted us to ask this question. The first involved a video of a seventeen year old (and therefore not involving child pornography) who performed a sex act at a public concert and which was put on YouTube. The second involved a teenager making embarrassing comments while drunk which were not obscene or offensive but were, one would imagine, deeply humiliating for the maker. Neither young woman in these cases could have had an expectation of privacy since both the events occurred in public. The question is whether a single upload of such material ought to be criminalised or whether existing civil remedies to have the material removed or for damages for an interference with privacy would be preferable and sufficient.

The question proved quite controversial. Responders observed that it would be difficult to define the offence where there was no expectation of privacy; that it should be technology neutral taking account of the usual approach of the criminal law to the actions of the defendant and their impact on the victim and not to the tools used to commit the offence; that much of this behaviour is already caught by existing offences; that civil remedies are more appropriate and in particular data protection remedies, and that there was a danger

that such an offence would excessively criminalise young people for posting "like" or other comments.

Others responded that they would prefer to see specific offences that would be more certain and that would not interfere to the same extent with free expression. They suggested enacting offences such as "voyeurism" (the old peeping Tom offence), or "upskirting", in order to criminalise the publication of intimate images or recordings including revenge porn. Examples of such offences can be found in Canada, England and Wales, and Australia.

Civil and criminal remedies

Many internet service providers have established their headquarters in Ireland. These include Skype, Facebook, Google, Yahoo, Amazon, Dropbox, Ebay, Paypal, Twitter, LinkedIn, and Ask.fm. Despite local availability of these internet companies, a major challenge to law enforcement in this area is jurisdictional: certain internet companies will hand over to the Gardaí on request content uploaded in Ireland but most will require the procedure established under the EU Convention on Mutual Assistance in Criminal Matters and the EU-USA Agreement on Mutual Legal Assistance, which can take up to eighteen months, before they will do so. Some claim that this is necessary because their servers are located overseas – usually California. We were informed that, in any event, children are reluctant to have the Gardaí involved and as a result there are very few criminal complaints. Where child pornography is placed on the internet platforms report it and remove it immediately.

Traditional court remedies for civil wrongs such as defamation which include injunction and damages, or for breach of the constitutional right to privacy are available in relation to wrongs committed on the internet. However, these have been shown in Ireland to be slow, expensive and in the end an empty remedy because what people really want is an early take-down of the offending material. Norwich Pharmacal orders to disclose an IP address can be sought where a posting is anonymous are not considered satisfactory either because they are also too slow and expensive for most. Respondents suggested that such orders should be able to be had from the Circuit Court (rather than the High Court); that there should be a one step process where an order revealing the IP address could be got both

from the intermediary and the telecoms company at the same time; that this remedy should be put on a statutory basis; and that anonymous users should be allowed to address the court before being identified as distinct from the current process which is *ex parte.*

The data protection regime has a lot to offer in this area. Data controllers, which include the internet service providers established in Ireland, are subject to the supervision of the Irish Data Protection Commissioner's Office. Data protection law has been harmonised and is enforceable across the European Economic Area and a new regulation is currently being negotiated. It protects individuals' rights to privacy regarding the collection, use and disclosure of personal data concerning an identifiable individual whether in the form of images, videos or other information. It provides remedies, both civil and criminal, and covers once-off incidents with harmful content. The basic rule is that where personal data is held by a data controller – which includes social networking sites and websites – the subject's consent is required where the data are processed. Individuals have the right to request removal or rectification of personal data and the Commissioner is provided with enforcement powers. However users who "[process] data in the course of a purely personal or household activity" are deemed not to be data controllers and this "household exemption" removes much material on social networking sites from the data protection regime. It is interesting to note certain decisions of the Court of Justice of the European Union (*Lindqvist* and *Rynes* which curtail the household exemption, and *Google Spain* which established the right to be forgotten) which suggest that it takes an expansive view of the duties of data controllers to protect personal data.

Specialist body

To address concern with court processes and remedies we asked in the Issues Paper whether there should be a specialist body to address complaints about material posted and most respondents were in favour. Such a body could offer mediation including take-down remedies and amicable settlement of disputes in a non-court setting. A majority of respondents supported the proposal but emphasised that it would have to be accessible, fast, cost effective, independent and, most importantly, provide effective remedies. Such a body would need adequate resources to fulfill what would likely be a busy remit. Such a

body was proposed by the New Zealand Law Commission and though it remains to be established legislation is currently proceeding through Parliament.

Extra-territorial jurisdiction for offences

Providing for extra-territorial jurisdiction for offences was considered to be desirable by most respondents. However introducing such jurisdiction is unlikely to make a large difference because it will either involve extradition or trial in absentia. Harmonisation of rules (possibly the data protection regime) and international agreements have more capacity to be effective. Even where different states have different standards concerning freedom of expression negotiation and enforcement of such agreements will, if possible at all, take time.

Public seminar

The Irish Law Reform Commission will host a public seminar on 22 May 2015. With the information gained there and from our consultations to date and any other responses that we may receive including from this group at the CALRAs Conference we will proceed to formulate a report which we hope to send to Government by the end of 2015.

END