SUBMISSION TO THE LAW REFORM COMMISSION

CYBER CRIME

FEBRUARY 2015

1.Whether the harassment offence in section 10 of the Non-Fatal Offences Against the Person Act 1997 should be amended to incorporate a specific reference to cyber-harassment, including indirect cyber-harassment

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?

Yes, for clarity harassment by cyber means should be included.

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?

No. To include "persistent posting online of harmful private and intimate material in breach of a victim's privacy" is very loose and not sufficiently aligned with criminal conduct as normally understood. Its closest kin is the section 10 offence which, if redefined so as to include indirect harassment, renders the use of the phrase "posting private and intimate material" unnecessary. It is the persistence, coupled with the harm, that creates the offence, not the intimate nature of the material. In terms of criminal conduct, the current understanding of what is intimate or private is not necessarily an easily identified concept. The suggested provision could become a significant redefinition of unwelcome or unexpected use of shared materials. To deem the distribution of material criminal without carefully defining the context and considering the potential for unfairness or lack of criminal intent would be rash. This is particularly incongruous (when one considers the current law) if the material was original freely shared. Does it become criminal conduct when shared with a person who already has it or only when shared with the wrong person? At what point does it become a criminal wrong, if it is the number of recipients which renders the conduct criminal? This suggested provision is not sufficiently clear in terms of its intent or its potential to constitute an appropriate addition to the criminal law.

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?

Yes. This is an important consideration due to the transnational nature of much internet communication. The alternative of relying on the law in the host state may not be satisfactory in all cases. It also circumvents the technical difficulties of identifying a host state in circumstances where a number of entities may be involved.

2.Whether there should be an offence that involves a single serious interference, through cybertechnology, with another person's privacy

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?

If section 13 of the Post Office (Amendment) Act 1951 (as amended by the Communications Regulation (Amendment) Act 2007) is to be amended to include electronic communications in the definition of measures dealing with the "sending of messages which are grossly offensive, indecent, obscene or menacing", this obviates the need for such an offence.

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

Yes.

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?

No. Any further reforms in this area would undesirable as there is a risk that the area could become over-criminalised. An amendment of section 13 should be sufficient to encompass the most serious breaches. Other behaviour which affects reputation is more appropriately dealt with through civil remedies.

We do not consider criminal sanctions for the host of such materials to be appropriate. Given that this is an area in which there is significant room for misunderstanding, the lack of clarity and potential for unfairness again mitigates against using the criminal law where it is unnecessary. The most important and effective remedy in such a case is the removal of the material and criminal sanction is not necesssary to achieve this.

3.Whether current law on hate crime adequately addresses activity that uses cyber technology and social media

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?

Yes. These acts are broad enough to encompass online hate crime activity. However, the position paper notes the difficulties with online hate speech compared to its offline equivalents. "Once an abusive comment is made it can spread very fast, be viewed by many people and remain accessible long after the content was posted." This is something which will be borne in mind by a sentencing judge after a successful prosecution under either of these acts.

4.Whether current penalties for offences which can apply to cyber-harassment and related behaviour are adequate

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

Yes. The current sentencing parameters for all of the legislation in question in this paper is already very broad and ranges from fines up to lengthy periods of imprisonment. The extent to which the material was disseminated online or otherwise is a matter for the sentencing judge and should be considered as factor, whether aggravating or mitigating, depending on circulation of the material. While some material may be widely circulated through no direct act of an accused, the criminal law already provides that circumstances which are foreseeable but not necessarily desired may be treated as aggravating factors. Mandatory minimum sentencing should be avoided.

5.The adequacy of civil law remedies to protect against cyber-harassment and to safeguard the right to privacy.

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?

Yes. The nature of online communications and the ability to disseminate potentially damaging information within seconds means that the availability of an immediate and effective remedy is crucial. Interlocutory injunctions should be granted more readily in cases of online defamation. However, as has been demonstrated by the McKeogh v Doe [2012] IEHC 95 case, interlocutory injunctions are not always as effective as they are

intended to be. This is a problem which needs to be addressed. Swift and effective access to "take-down" orders is desirable in appropriate cases.

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?

It is clear that the proliferation of internet communications and cybercrime means that certain court procedures, particularly in relation to discovery, need to be adapted to recognise and accommodate the vast remit of cyber interactions. The anonymity of the internet is a powerful force which makes it much more difficult for a victim to identify a wrongdoer. The recommendations of the 2014 Report of the Internet Content Governance Advisory Group are progressive, particularly with regards to easier access to Norwich Pharmacal orders. However, with the increasing need to adapt pre-trial procedures relating to "cyber-discovery", comes an concomitant need to ensure that freedom of expression and the right to privacy is afforded a similar level of protection. The balance between these competing rights needs to be adequately considered.

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?

Yes. In certain suitable circumstances, this could be an effective method of dealing with cases without having to engage in litigation. This specialist body could particularly assist victims in obtaining a "take-down" order in a speedy manner. As the issues paper points out, this can only be done where the wrongdoer is "identifiable and cooperative". However, the constitutional right to freedom of expression would need to be afforded adequate safeguards.

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?

Although some action has been taken to address problems of recognition and enforcement within the EU this is still a significant problem outside of the EU. This problem is not unique to cybercrime. The nature of internet communications, with its inconstant and fluctuating borders, means recognition and enforcement of judgments in this area will be a significant issue in the future.