**Predict Conference Dublin 17 September 2015**

**Insight Workshop: Bill of Rights for Digital Age**

**Pauline Walley SC[[1]](#footnote-1)**

**Introduction.**

It is a great pleasure to address you this morning as part of the Predict 2015 Conference on the legal challenges which face citizens in the online world, in terms of privacy infringement, damage to reputation and cyber harassment.

My talk is divided into four parts. In Part I, I would like to focus on why cyber is different in a rights context, and to highlight this by giving some examples of the new forms of abuse such as online harassment, revenge porn and trolling which affect citizens in the digital environment. In Part II, I talk about how existing legal remedies are grossly inadequate to deal with many of these issues, as current laws were framed often in nineteenth century for entirely different scenarios. In Part III, I talk about what is the primary issue for most victims of cyber abuse- whether that is online defamation, harassment or trolling, and that is the vexed issue of take downs and keep downs. I touch on the recent *Google Spain* decision, which was delivered in the context of EU data protection laws. In the concluding part IV, I focus on the need for a multi layered approach to these issues. We need bespoke cyber laws to effectively deal with unlawful activity, as well as procedural laws on proofs in civil and criminal litigation. But we also need structures which underpin the rights of citizens before they get to the doors of a court. In other words, we need a Bill of Rights which sets out what each citizen is entitled to in terms of protections of their fundamental privacy and reputational rights and interests within the online space, as well as clear procedural rules and guidance regarding take downs to include focussed time limits, as well as a tiered process for dispute resolution.

1. **Background**

Advances in technology have enhanced our lives, and rendered global communication accessible to most of society in a way never previously contemplated. Information has become freely available in a way which has transformed how we, as human beings, live, work, communicate and interact with each other. New inventions have undoubtedly made our lives easier, albeit faster, but such innovations also have a potential downside, if that technology is used to transmit or communicate material which harasses a citizen, or which peddles defamatory material, thereby ruining reputation, livelihood and possibly security, or which destroys in a culpable manner the peace, security and autonomy of the individual.

Many academic commentators argue that the challenges posed by internet abuse simply requires a “cyber gloss” on existing analogue laws, so as to ensure the protection and vindication of rights such as good name, reputation, privacy and security. This is, in part driven by the understandable desire to promote free speech in an online environment, which is rightly regarded as a core component in the underpinning of democracy, and to interfere, as little as possible, with current laws. But as expert legal commentators such as Keats Citron and Solove have pointed out, this conceptual approach misunderstands the nature of cyber damage, and how bespoke cyber laws are required to meet the real challenges posed by this new cyber environment. They argue that the digital space, if left unchecked, risks encouraging a feral environment where cyber mobs reign supreme.

It must be remembered that free speech, like privacy, is not an absolute right, and that all common law jurisdictions proscribe speech in a number of ways, so as to outlaw, for example, child pornography, treason, defamation, breaches of official secrets or criminal contempt laws. These are all manifestations of “speech”, yet society values competing rights such as the protection of children, the security of the State, the protection of good name, or the integrity of a trial process as deserving of protection, and thereby limits free speech in those specified circumstances. In other words, there is a countervailing right or social good, which society deems meritorious of protection.

We are now at a legislative cross roads, where we as a society, and our lawmakers, must count the social cost associated with the downsides of these great new technologies, or rather, the negative human behaviour which such technologies enable. This is not a new process, nor is this a paean to Luddite values: with the advent of the printing press, copyright laws were enacted: with the advent of the Industrial Revolution, laws regarding child labour, Factories Acts and health and safety legislation followed: with the advent of the motor car, road traffic laws evolved. In other words, each new technological advance and accompanying sociological shift in society spawns new laws. There is always a period of transition or *inter regnum*, where stakeholders debate the necessity, or otherwise, of new laws. The dilemmas of the cyber revolution are no different. In the case of internet abuse, our challenge is to recalibrate new laws for this new digital space, and to elucidate where the dividing line is between cyber rights and cyber responsibilities.

1. **How Cyber damage is Different, and Needs Bespoke Cyber Laws**

The simple “cyber tweak” approach advocated by some commentators to the amendment of existing domestic harassment laws is to fundamentally underestimate the nature of cyber- harassment, and how it is different from off- line harassment. The nature of the damage is different: it is published globally, and not locally. It is published in a permanently recorded and accessible manner; forever in the ether, as one judge remarked, like a digital tattoo on one’s reputation and good name. The material is often anonymous, and may include hate speech. It may incite others to troll the victim. The infringing material may travel to other sites by hyperlinking and file sharing, and may become viral. It may also be interactive on websites and social media platforms.

It is also the case that, unlike most cases of off line harassment, online harassment often involves children- sometimes hailed as the digital natives in our society- as the tragic teenage suicide cases of Erin Gallagher and Ciara Pugsley demonstrate, where the scale and reach of cyber bullying/harassment is totally different to offline abuse. Indeed, one of the significant features of cyber abuse of children is that the very devices which parents give to their children to be safe, i.e. a mobile phone, is very often the device which is used by cyber bullies to follow, harass and oppress the child. To suggest that children such be compelled to abandon the use of such devices, as some kind of prophylactic response to cyber bullying or harassment, is naïve. The essence of the digital age is connectivity for both adults and children alike.

It is also argued by many experts that the psychological “fall out” from this type of harassment is both different, and enhanced. Cyber experts around the world are still trying to assess why the impact is greater, and how we as a society might deal with these social costs. But if the impact is significant, as these experts suggest, then society must consider how best to mark the seriousness of this type of misconduct, and how to develop not only norms, but incentives, for citizens to regulate their behaviour in an appropriate way.

There are additional technical challenges presented by online abuse which are not present in an offline context. Whilst the original uploader may ultimately be persuaded to take the unlawful material down, if the material has travelled and become viral, the only entity which can effectively take the harassing or defamatory material down is the internet intermediary (“ISP”). In other words, unlike traditional torts, it is not just a simple model of victim and perpetrator, and how society defines the rights and the responsibilities of both, *inter partes*.

In a wider context, the issue of personal privacy and autonomy has achieved significant prominence with the Edward Snowden revelations of the NSA trawl through our personal data. The extent and nature of the material copied to government agencies without our knowledge or consent comes as a real shock to us in Europe who are accustomed to a certain level of privacy and data protection rights. The Snowden revelations have raised serious questions for individuals and society as a whole on the interconnected issues of privacy and security. The key questions are what is actually happening to our data and who has access to it. There is a profound mistrust on the part of most citizens as to what is happening to their data. Most citizens feel that when they turn on their mobile in the morning, they are in a sense engaging in a Faustian pact with service providers in relation to their privacy and autonomy rights. We want what the technology can give us in terms of reach and access. We do not want to be surveilled and tracked, and we just hope-blindly perhaps- that those commercial entities to whom we give our data, will not betray us. In a Big Data and Predict context, that lack of trust on the part of data subjects is one of your great challenges.

 *Examples of Online Defamation and Cyber Harassment.*

* Online defamation: *Hegglin v Google Inc.* in UK; in Ireland, *McKeogh v Doe 1 and* *Others,* Peart J. High Court, May 16, 2013
* Harassment and defamation via fake profiles on platforms like Facebook: *R v Debnath.*
* AutoAdmit Case in U.S.- group attack on 39 female law students
* Rise of revenge porn, and abuse of intimate selfies, as in *Wilson v Ferguson* [2015] WASC 15.

1. **Existing laws are inadequate**

Although there are existing statutes in relation to harassment and defamation, these laws were framed for a society and a way of living which no longer exists.

Harassment in cyberspace is different. It is often based on the perpetrator publishing the name, address, mobile and social security numbers of the victim online, and inviting unknown third parties- who have no connection with the victim- to stalk or troll the victim. Very often, the troll activity, such as sending an abusive tweet may be perfectly lawful, but if 2-3k tweets are sent in a day, this may become unlawful as in the Criado Perez case. The perpetrator may also invite third parties to rape the victim suggesting that the victim is consensually available for such activity, as in the case of *R v Da Silva* in Canada. Although the Non-Fatal Offences against the Person Act 1997 does contain an offence of harassment which relates to the watching and besetting of a person, this requires a persistent course of conduct. A single upload to a website inviting third parties to troll and pass it on would simply not be covered. Furthermore, the Act requires proof regarding the intent of the perpetrator, and his likely knowledge of the effect of the abuse on the victim. If there is a real disconnect between the perpetrator and the victim, the law as it is currently framed just cannot deal with these types of factual scenarios.

In an online defamation context, the immediate priority for the victim is takedown. If the poster refuses to take the defamatory material down, or the poster is anonymous, the victim has real problems as they are likely to face weeks, months, years of waggling with search engines and websites trying to take it down, but also to keep it down, as in the *Hegglin* and *McKeogh* cases.

In a privacy context, the case of Max Mosley demonstrates you can win in court with your privacy action- in his case the News of the World in 2008, but the thumbnails in Google cache were still showing the images of private sexual activity for years after a High Court judge had said such photographs were a gross invasion of his privacy rights. He spent seven years fighting with Google in various parts of Europe re takedowns, arguing privacy and data protection rights, which were ignored until they settled his case earlier this year on a confidential basis. Most citizens do not have either the financial or physical resources to sustain such arduous litigation, and should not be required to do so.

In addition, our laws are utterly outdated on issues such as to how you prove postings on an international platform for the purpose of civil and criminal litigation, and how you deal with trans-border jurisdictional issues.

The issue of the E Commerce Directive 2000/31/EC also needs urgent review as the Directive is hopelessly out of date. The ECD conferred qualified immunity in damages claims on ISPs for unlawful third party content, providing they removed same once they were put on notice of the unlawful nature of the content. This has encouraged some ISPs to be quite resistant to the issue of notice, and opaque in their responses. Our EU lawmakers failed to bring in a Notice and Takedown procedure to accompany the Directive- which should manifestly have been implemented as a concomitant *quid pro quo* for qualified immunity- which has left citizens whose lives and reputations are ruined by online abuse, often to the mercy of private law remedies.

So we need bespoke cyber laws to deal with these issues. They cannot be framed in an over broad way, and we must make a clear distinction between material which is merely offensive- which is perfectly lawful, and material which is used to harass or defame, and thereby unlawful. Free speech matters, but feral free speech renders us all less free and the captive of a mob.

1. **Takedowns and *Google Spain***

The role of the internet intermediaries (ISPs) is also vital in terms of achieving takedown of unlawful material, and this is a vexed issue. Prior to the dicta of the CJEU in the case of *Google Spain*, many victims of unlawful cyber abuse contended that it was almost impossible to persuade the ISP to take material down. If -as in the case of *Hegglin* or *Mosely*, you are the victim of cyber abuse, it matters little that you may have a damages claim against the perpetrator. What you want is immediate takedown; a damages claim is often an irrelevant or unrealistic issue. The trouble is the only entity which can achieve takedown is the ISP, and persuading them to take material down can be difficult.

In May 2014, the CJEU delivered its judgment in *Google Spain* [[2]](#footnote-2)which determined that- in a data protection law context- personal data which is out of date, irrelevant or places a person in a false light should be de-indexed from search engines. The material could still be available on the newspaper site, or other websites. The decision affected search engines only. In the course of its judgment, the court laid heavy emphasis on the importance of Arts. 7 and of the Charter of Fundamental Rights, which has elevated data protection rights within the EU to a constitutional status post- Lisbon Treaty in December 2009. In the immediate aftermath, Google decried the decision as a form of censorship, but guess what? Twelve months later, the dust has settled. The sky has not fallen in, and Google in their Transparency Report in 2015 say they have only acceded to about 49% of requests. Despite the grim predictions of the search engines, free speech is still alive and well, protected by excellent journalists and print media such as the Guardian newspaper, which revealed the true position on that Transparency Report.[[3]](#footnote-3)

Yet despite the strong dicta by the CJEU in *Google Spain*, and the General Data Protection Regulation which is expected to become law- and directly effective in late 2015- it is the view of some practitioners that it is still difficult to persuade ISPs to take material down which is either unlawfully harassing or defamatory, as is demonstrably clear from recent case law in both Ireland and England.[[4]](#footnote-4) In other words, some practitioners and experts such as Leiter argue that the absence of unambiguous black letter law on these issues, both in the context of the perpetrator of the infringing upload, and in terms of the inactivity of the ISP on takedown and keep down requests (which are separate and distinct issues), act as an incentive to perpetuate this cycle of abuse. The *Google Spain* ruling only applies to personal data as defined, which is an important distinction, and demonstrates that DP laws cannot cover every scenario of online unlawful abuse. In addition, the search engines will only take the material down within the EU, so it is still available worldwide, or through the .com portal. The ISPs also will not monitor their platforms/sites to ensure that the material will not be uploaded again saying that this is general monitoring contrary to the E Commerce Directive 2000/31/EC, so victims must continue to trawl the internet themselves indefinitely, so that they can nominate further URLs as they discover them. This is despite the fact that the E Commerce Directive specifically acknowledges that courts may grant injunctions to both “terminate” and “prevent” infringement. The word “prevent” clearly applies to a keep down scenario. For an abuse victim, this scenario is worthy of the novels of Kafka. In addition, the culpable failure of the EU to provide for, and implement, an EU wide Notice and TakeDown procedure has forced many plaintiffs-in the absence of such a basic and fundamental structure- to try and re-fashion their claims into a data protection claim, thus inundating data protection commissioners throughout Europe with DP claims.

1. **Multi layered Approach and Bill of Rights**

So we must as a society consider how far the law can or should go to in terms of calibration of rights, sanctions and takedowns. There is a clear dividing line between the freedom of expression rights of the individual poster or the cyber mob (constitutional right, Article 10, Charter, First Amendment rights), versus the countervailing constitutional, ECHR and Charter rights of privacy data protection and dignity of the victim.

In my view, citizens-no matter where they reside-should be entitled to the following from ISPs, no matter where they are located:

1. A well-defined Notice and Take Down Procedure, with strict time limits and real time human point of contacts. There is no reason why an inittial human response turn-around of 24 hours, which in internet terms is an infinity, could not be achievable;
2. A requirement that if a complaint has not been resolved within, say 48 hours, that it is passed to a dispute resolution/mediations service-paid for by way of levy on the ISPs who contribute to a general annual DR fund. This service should also have a strict time limit, so that if matters are not resolved within say- 7 days- the complainant can refer the matter to a technology division of the Circuit or High Courts.
3. ISPs could consider the use of a takedown escrow, for a short duration-say 2-3 days, whilst reviewing a complaint. Their very widely drafted Terms and Conditions would permit this.
4. Victims and posters should have immediate access to courts for injunctive relief regarding take downs if the ISP is not prepared to place the post(s) in escrow, and for rulings, or if the poster wishes to prevent take down justifying public interest etc.
5. Costs should be capped for both Circuit and High Court.
6. A court should be able to grant permanent injunctions regarding specific material, rather than on a specific URLs basis. Court do have an inherent jurisdiction to grant such orders, but it perhaps needs to be spelled out in view of the ISP arguments that “keep downs” constitutes general monitoring contrary to the E Commerce Directive 2000/31/EC.
7. Ireland is ideally placed to locate this type of tiered legal/dispute resolution service as most of the major ISPs are located here, and many of them have adapted their T & Cs to be governed under Irish law. Furthermore, our flexible, “can-do”, problem solving mentality is ideally suited to find human based solutions.

Finally, all of this should be underpinned by a Bill of Rights in a digital context, which should re-affirm the fundamental principles of essential dignity, privacy and autonomy of each citizen in a global cyber context, which principles underpin both our laws, and our commitment to the rule of law.

In June 2015, the common law world celebrated the 800th anniversary of the signing of Magna Carta at Runnymeade. Although the Charter was later amended, repealed and resurrected in various guises, the fundamental principles which it enshrined are still with us today- the protection of liberty, habeas corpus and trial by jury. It was these guiding principles which later informed all major human rights instruments and the Bill of Rights. We need a Magna Carta for the digital age. As we face new challenges with the Internet of Things, artificial intelligence, and a world where we risk de-skilling as we cede some human autonomy to the machine age, we need to re-imagine what matters about being human. We need to ask ourselves what the words dignity, privacy and autonomy really mean in this brave new world, whilst preserving fundamental free speech values. We need to ensure that all our citizens- world-wide-are afforded nothing less in the digital space.

1. ©Pauline Walley SC is a practising barrister with a general practice in civil, criminal and internet litigation. She is the co-author of *Cyber Law and Employment* to be published by Roundhall Publishers, Dublin late 2015. [↑](#footnote-ref-1)
2. *Google Spain SL v Agencia Española de Protección de Datos (AEPD) (C-131/12), Grand Chamber, May 13, 2014.* [↑](#footnote-ref-2)
3. Julia Powles “*Google accidentally reveals data on “right to be forgotten” requests”* The Guardian July 14, 2015. [↑](#footnote-ref-3)
4. *McKeogh; Mosley; Hegglin.* [↑](#footnote-ref-4)