# Submission to the Committee on Justice and Equality on *issues of online harassment, harmful communications and related offences.*

Éibhear Ó hAnluain

September 20, 2019

## 1 Introduction

My name is Éibhear Ó hAnluain and I have been working in software engineering and IT systems design since 1994. I thank you for the opportunity to submit this contribution to your analysis of *issues of online harassment, harmful communications and related offences.*

In this submission I am seeking to highlight 2 core concern

- The nature of the online services from the perspective of small operators
- The potential damage legislative measures can have on small operators of online services

I will also address some additional concerns I believe are relevant to this analysis.

### 1.1 Summary

1. *Self-hosting* is where an individual, a small group or a small business manages their own online service, rather than making use of a third-party service. There are self-hosting alternatives to all of the major services that would be under consideration for your analysis. In recent years, legislation enacted out of Europe and around the world that seeks to control expression online seems to regard only the large organisations, and can severely inhibit innocent self-hosting activities by applying additional burdens on the service operators.

   I maintain a set services for my own purposes, or to allow me to connect or collaborate with family and friends on my own terms, and I believe that these activities are at risk from poorly drafted legislation.

2. Legislation and regulations that allow for user-posted material to be taken offline are often abused. A regime that punishes a service operator for

leaving alleged infringing or illegal material up but that doesn't sanction the operator for taking down innocent material will result in significant infringement of internet users' speech rights with no consequences for the service operator or those alleging infringement or illegality.

3. *Content Moderation* is the process whereby service operators decide whether material can stay on the service or not. It is very hard to do right, and is impossible to do it at scale. Assertions that service operators are "doing nothing" are wrong on the face of it and ignores the challenges involved.

4. It is the behaviour of users, and the decisions of users that results in bullying, harassment and harmful material online. Very few services, and none of the large services, encourage or want their system to be used for this purpose.

5. Requiring that material be taken offline without regard for the consequences of doing so can be dangerous. In particular, if a crime has been committed, it may necessary to preserve a posting in order to allow for it to be presented as evidence in court.

6. Encryption is not something that should be interfered with by legislation. There is a wide body of expertise and experience showing this to be the case. Interfering with encryption services will only have no effect on those who want to use encryption for illegal activities but will have a devastating impact on innocent people.

I make the following recommendations in this submission:

1. Laws that seek to control online materials should take into consideration that ability of all legal, innocent services to implement required measures. Overly burdensome rules will result in the loss of many valuable services while cementing the market positions of the services that have the financial resources to implement the rules.

2. Laws that seek to control online materials should punish severely attempts to abuse them to stifle free expression and remove innocent material.

3. While *self-regulation* has a bad reputation, it is imperative for legislators to examine in detail how services are dealing with harmful and abusive material and to consider the challenges involved.

4. Laws should target user behaviour more than seek to punish third parties.

5. To protect free expression includes ensuring that material that is considered illegal is made available to those who investigate human rights abuses.

# 2 Self-hosting

## 2.1 Self-hosting

For the purposes of this submission, *self-hosting* is where an individual or small group has opted to provide their own internet services, making use either of computer capacity provided by an ISP (for example, Blacknight.com, Amazon AWS) or by maintaining the underlying computer technology themselves.

The services that the self-hoster exposes, then, are either developed specifically by the self-hoster or runs software that has been installed by the self-hoster.

The self-hoster also takes responsibility for the quality of the service that they provide, including ensuring that it is kept running and updates are applied appropriately, and so on.

A list of services that can be self-hosted, and the software packages that can be used for those services is available at `https://github.com/Kickball/awesome-selfhosted`.

This submission is primarily concerned about self-hosting as a hobby and self-hosting engaged in by charity, non-governmental or community organisations. However, self-hosting for commercial purposes is a valid use-case, but implications of regulations on self-hosting has more a direct implication on the former use-cases, as the effect of poor regulation on vulnerable people would be more direct, immediate and serious.

### 2.1.1 Real examples of self-hosting

I host a number of services:

- *Éibhear/Gibiris* (http://www.gibiris.org/eo-blog) is my blog site.
- *Social Gibiris* (https://social.gibiris.org/) is a micro-blogging service that is federated with others using the *AtomPub* technology. Thus, *Social Gibiris* is federated with many other instances of *GNU Social*, *Mastodon* and *Pleroma*. This network of federated services, operated by individuals, groups and businesses, all connected together as peers, facilitate connections and communication in a way that is very little different to twitter.
- *git.gibiris.org* is a source-code sharing site that I use to make publicly available some of the software that I develop for myself.
- *news.gibiris.org* is a news-aggregation service that allows me to gather all the news sources of interest to me into one location, which I can then access from wherever I am.
- *cloud.gibiris.org* is a file-sharing platform that I use with my family when we are collaborating on projects (e.g. school projects, home improvement projects, etc.)
- *matrix.gibiris.org* is an instant-messaging system which I set up for the purposes of communicating with my family and close friends.

Most of these services are hosted on a computer within my home. 3 of these services provide information to the general public, and the other three are accessible only to those who set up accounts.

2 of those services, *git.gibiris.org* and *Social Gibiris* can process or post user-uploaded information.

### 2.1.2 Why self-host?

There is a myriad of reasons for choosing to host one's own service. Some examples might be:

- Privacy – until recently many of the most popular services were careless or outright abusive users' privacy
- Tracking – many organisations, particularly those whose business models are based on advertising, facilitate the tracking of internet users as they conduct their business or personal activities across the internet.
- Autonomy – to be able to configure ones own service is often a powerful experience.
- Community – While some of the global services with household names offer features to small businesses and community groups (like football clubs or debating societies), often the lock-in and exclusivity involved can make it hard to include everyone who needs to be included. Hosting your own services allows you to set the rules and codes of conduct appropriate for your groups specific needs.
- Experimentation – just by means of playing with interesting software projects can people often learn about the tools and systems they use, and grow their knowledge of the technologies involved.
- Collaboration – the software that implements self-hosted services often come under the terms of a Free or Open Source Software copyright licence, which allows for people to copy and improve the software, and these improvements often find their back to the original project for others to benefit.
- Protection – Governments in countries where civil rights are not regarded as highly as they are in Ireland very often delight in the greater ease involved in surveilling their populations when the records of all that activity are centralised in a single service.

Very often, as with me, the reason to self-host is a combination of more than 1 of these reasons.

## 2.2 How accessible is self-hosting.

In a previous, similar, submission[1], I provide an outline of the challenges before someone who wants to set up their own services. They are few, and they are small. In summary, the reasons for this are:

- The Internet is mechanism for computers to find each other and then to share information with each other. The mechanism is defined in a set of publicly-available documents describing the relevant protocols.
- Due to the maturity and age of these protocols, software needed to use them is now abundant and trivially easy to get and install and run on any general-purpose computer. Such software is also very easy to develop for moderately-skilled software engineers.
- Neither the protocols that define, nor the software that implement the internet regard any computer to be superior or inferior to any other computer. For this reason, there is no cost or capacity barrier to running an internet service: if you have the software, and the internet connection, then you can expose an online service.

Clear examples from the past of how the accessibility of the internet technologies has benefited the world include the following:

- The *Linux* operating system kernel began life in 1991 as a college project – Linus Torvalds wanted to write a computer operating system that was accessible to all. Linux-based operating systems now form the basis of a significant proportion of internet connected computing devices globally[2] (including 73% of smartphones and tablet computers, somewhere between 36% and 66% of internet-facing server computers), and 100% of supercomputers.
- The *Apache* web server started development when a group of 8 software developers wanted to add functionality to one of the original web server software packages, *NCSA httpd*. The Apache web server now powers 43.6% of all web sites[3].
- The *Firefox* web browser was initiated by three software developers who wanted to make a light-weight browser based on the Mozilla code-base. At the height of its popularity, *Firefox* was used in 34% of web-page requests, despite not coming installed by default on any computer or mobile device. However, its real impact is that it was instrumental in breaking

[1] Available here (http://www.gibiris.org/eo-blog/posts/2019/04/15_harmful-content-consultation.html) and here (https://www.dccae.gov.ie/en-ie/communications/consultations/Documents/86/submissions/Eibhear_O_HAnluain.pdf).

[2] *Usage share of operating systems* (https://en.wikipedia.org/wiki/Usage_share_of_operating_systems)

[3] *Usage of web servers* (https://w3techs.com/technologies/overview/web_server/all). Incidentally, the no. 2 on that web page, with nearly 42% share of websites is *nginx*. It also started out as a project by an individual who wanted to solve a particular project.

the monopoly that Microsoft's Internet Explorer held since the late '90s, resulting in far richer and more secure web.

When we look at the main services that society is currently struggling with, we need to consider the following historical facts:

- Facebook started out as a crude service, developed in Mark Zuckerberg's room in Harvard University, to allow users (men, of course) to rate the women in the university in terms of "hotness".
- Google started out as a search engine called "Backrub". Development initially took place in a garage.
- eBay was originally an auction service tagged onto the personal website of its founder, Pierre Omidyar.
- LinkedIn was initially developed in Reid Hoffman's apartment in 2003.
- Shutterstock, a leading provider of stock images, was founded by a photographer, John Oringer, who developed the service as a means to make available 30,000 of his own photographs.

The ease with which internet technology can be accessed is instrumental in the explosion of services that connect people, and people with businesses.

It is critical to note that many of these technologies and services started out with an individual or small group developing an idea and showing it can work **prior** to receiving the large capital investments that resulted in their current dominance.

All of the above technologies and services can be considered truly disruptive. In their respective domains, their arrivals resulted in a dramatic improvements in internet technologies and services.

However, There are many alternatives to the systems that we are familiar with, all developed by individuals, or small, enthusiastic teams:

- *Twitter* isn't the only micro-blogging service: there's also *GNU Social*, *Pleroma*, *Mastodon*.
- An alternative to *Facebook* is *diaspora**
- *Nextcloud* and *Owncloud* are examples of alternatives to *Dropbox*.

In the cases of all these alternatives, users can sign up for accounts on "instances" operated by third-party providers, or users can set up their own instances and operate the services themselves.

Many of these services can federate with others. Federation in this context means that there can be multiple instances of a service, communicating with each other over a defined protocol, sharing updates and posts. For users, federation means that they can interact with other users who aren't necessarily on the same node or instance. For administrators of instances, federation means that they can configure their instances according to their own preferences, rather

than having to abide by the rules or technical implementation of someone else. For the ecosystem, federation means that if one node goes down or is attacked, the others can continue with a minimum of interruption.

### 2.3 Regulation of self-hosted services

While it is attractive to create regulations to manage the large, profit-making organisations, it is imperative that such regulations don't harm the desire of those who want to create their own services.

A regulation that applies liability to a service-provider for someone else's behaviour is a regulation that can be adhered to only by organisations with large amounts of money to hand. For example, if the regulation was to apply liability on me for a posting made by someone else that appears on one of the services that I run (and likely originally posted **somewhere** else – these are federated services after all), I would have to shut it down; I am not able to put in place the necessary technical or legal infrastructure that would mitigate my liability[4]. Given that my services are intended to provide a positive benefit to me, my family members and my friends, and that I have no desire to facilitate harmful behaviour on these services, a law forcing me to shut these services down benefits no one.

Similarly, a regulation that demands responses from services on the assumption that the service will be manned at all times, requires individuals who are self-hosting their services to be available at all times (i.e. to be able to respond regardless of whether they are asleep, or overseas on a family holiday, too ill to respond, etc.)

This submission comes from this perspective: that small operators should not be unduly harmed by regulations; the likelihood of this harm coming to pass is greater when such small operators are not even considered during the development of the regulations. If regulations have the effect[5] of harming such small operators, the result will not just be the loss of these services, but also the loss of opportunity to make the Web richer because artificial barriers to entry will be imposed by those regulations. They will inhibit the development of ideas that pop into the heads of individuals, who would realise them with nothing more than a computer connected to the internet.

## 3 Other considerations

While the main focus of this submission is to highlight the potential risk to self-hosters from regulations that neglect to consider the practice, I would like to take the opportunity to briefly raise some additional concerns

[4] This assumes that my services aren't forced to shut down by the new EU Copyright Directive anyway

[5] unintended, one hopes

### 3.1 Abuse of the systems

To date, all systems that seek to protect others from harmful or other objectionable material (e.g. copyright infringement, terrorism propaganda, etc.) have been easily amenable to abuse. For example, in a recent court filing, Google claimed that 99.97% of copyright infringement notices it received in from a single party in January 2017 were bogus[6]:

> A significant portion of the recent increases in DMCA submission volumes for Google Search stem from notices that appear to be duplicative, unnecessary, or mistaken. As we explained at the San Francisco Roundtable, a substantial number of takedown requests submitted to Google are for URLs that have never been in our search index, and therefore could never have appeared in our search results. For example, in January 2017, the most prolific submitter submitted notices that Google honored for 16,457,433 URLs. But on further inspection, 16,450,129 (99.97%) of those URLs were not in our search index in the first place. Nor is this problem limited to one submitter: in total, 99.95% of all URLs processed from our Trusted Copyright Removal Program in January 2017 were not in our index.

With the US' Digital Millennium Copyright Act, there is no downside for a bad-faith actor seeking to take advantage of a system for suppressing information[7].

The GDPR's *Right to be Forgotten* is also subject to abuse. An individual from Europe continues to force stories related to him excluded from Google searches. However appropriate on the face of it, the stories this individual is now getting suppressed relate to his continued abuse of the *Right to be Forgotten*[8]. That the "right" can be abused in this way is counter to the public interest, as it can now be used like a "Super Injunction".

While the GDPR allows for search engines "... exercising the right of freedom of expression and information", if they are presented with *Right to be Forgotten* demands, they have to choose between serious sanctions if they don't filter the results when they should have, or no sanctions if they suppress the results when they didn't need to.

In systems that facilitate censorship[9], it is important to do more than merely assert that service providers should regard fundamental rights for expression and information. In a regime where sending an e-mail costs nearly nothing, where

[6] *Google Report: 99.95 Percent Of DMCA Takedown Notices Are Bot-Generated Bullshit Buckshot* (https://www.techdirt.com/articles/20170223/06160336772)

[7] The law contains a provision that claims of copyright ownership on the part of the claimant are to be made under penalty of perjury. However, that provision is very weak, and seems not to be a deterrent for a determined agent: *Warner Bros: Our False DMCA Takedowns Are Not a Crime* (https://torrentfreak.com/warner-bros-our-false-dmca-takedowns-are-not-a-crime-131115)

[8] `https://www.techdirt.com/articles/20190320/09481541833`

[9] While seeking to achieve a valuable and socially important goal, legislation of this nature facilitates censorship: as a society, we should not be so squeamish about admitting this.

a service risks serious penalties (up to and including having to shut down) and where a claimant suffers nothing for abusive claims, the regime is guaranteed to be abused.

## 3.2 Content Moderation

Much of the focus of legislative efforts to deal with harmful or objectionable material that appear on services that permit uploads from users is on what the service providers do about it. Many argue that they are not doing anything, or at least not enough.

However, this is an unfortunate mischaracterisation of the situation. For example, facebook employs – either directly or through out-sourcing contracts – many 10s of thousands "moderators", whose job is to make a decision to remove offensive material or not, to suppress someone's freedom of expression or not, based on a set of if-then-else questions. These questions are not easy:

- It's illegal in Germany to say anything that can be construed as glorifying the Holocaust. In the US it isn't. Facebook can suppress such information from users it believes are in Germany, but to do so for those in the US would be an illegal denial of free expression, regardless of how objectionable the material is. What is facebook to do with users in Germany who route their internet connections through the UK? Facebook has no knowledge of this unusual routing, and to seek to learn about it could be a violation of the user's right to privacy. Should facebook be criminally liable for a German user seeing statements that are illegal in Germany?

- Consider the genocide of Armenian people in Turkey in 1915. In Turkey it is illegal to claim it happened. However, for a period between 2012 and 2017 it was illegal in France to claim it didn't happen. In most other countries, neither claim is illegal. What can a service like facebook do when faced with 3 options, 2 of which are mutually exclusive? Literally, they would be criminally liable both if they do *and* if they don't[10]?

Moderators have no more than a minute to determine whether a statement complies with the law or not, and this includes figuring out whether the posting meets the definitions of abusive or harmful, and whether it is indeed intended to meet that definition. For example, consider an abusive tweet. Should the harmful, abusive tweet be removed? Who decides? What if the target of the abusive tweet wants that tweet to be retained, for, say future evidence in a claim? What if the tweet was an attempt at abuse, but the target chose not to be affected by it? Should it stay up? Who decides? What if the target doesn't care, but others who see the tweet and are not the target of the abuse may be offended by it. Should it be taken down as abusive even though the target of the

[10]Prior to his assassination in Istanbul in 2007, Hrant Dink, an ethnic Armenian Turkish journalist who campaigned against Turkey's denial of the Armenian Genocide had planned to travel to France to deny it in order to highlight the contradictions with laws that criminalise statements of fact.

abuse doesn't care, or objects to its removal? Who would be criminally liable in these situations? What if the target of the abuse substantially quotes the abusive tweets? Is the target now to be considered an offender under a criminal liability regime when that person may be doing nothing other than *highlighting* abuse?

All of these scenarios are valid and play out every day. Content moderators need to consider these and many more questions, but get very little time to do so. The result: a public perception, promoted by public figures, that these large services are doing nothing about abuse.

"Content moderation" is very hard, and is impossible at the scales that services like twitter or facebook operate in. When context is critical to decide that someone is engaged in harmful or abusive behaviour, it would be fundamentally unfair to make a service criminally liable just because it made the wrong decision as it didn't have time to determine the full context, or because it misinterpreted or misunderstood the context.

## 3.3 User Behaviour

Many believe that the way to deal with abusive or harmful material online is to punish the services that host the material. This is reasonable if the material was placed onto the service by those who operate the service. It is also reasonable if the material is put there by users with the clear knowledge of the service operator, or by users following encouragement of the operators of the service.

However, these specific situations are rare in the world of normal online services[11].

Engaging in harmful and abusive communications is a matter of behaviour and not a function of the technical medium through which the communication is made. The idea that internet services are responsible for abusive communications is as difficult to understand as the idea that a table-saw manufacturer is responsible for a carpenter not wearing safety glasses.

Recent history has shown that the most effective ways to change behaviour are not necessarily punitive. It's hard to see how punishing an intermediary would stop people being nasty to each other.

Any new regulations around controlling abusive or harmful behaviours online must start with changing user's behaviours. If there is no attempt to change behaviour, then abusive people will simply work around the controls and continue to abuse.

## 3.4 Investigation support

In response to the live-streaming of that horrific shooting dead of more than 50 people in New Zealand earlier this year, that country has declared the video

[11] Services that are dedicated to hosting criminal material such as "revenge porn" or child sexual exploitation material know they are engaged in criminal activities anyway, and take steps to avoid detection that are outside the scope of this submission – those guys will get no support from me!

recorded by that white supremacist terrorist as "objectionable", making it a criminal offence to share it[12].

While one can understand the thinking that sharing the material could only be done by people who support the atrocity, this is not necessarily true. Other reasons to share the video or portions of it might include

- to appeal for help in finding someone caught up in the massacre
- legitimate news reporting of such an event.
- to help investigate the shooting and its circumstances[13]
- training for law enforcement or terrorism- or disaster-response personnel.

However, if the law says that no form of sharing is permitted, then none of the entirely legitimate purposes would be possible, and the world would be that bit less safe as a result.

There is a similar consideration for abusive material posted online. If a communication is deemed to be an offence, care needs to be taken to ensure that the "removal" of such a communication (or a set of such communications) is not equivalent of the destruction of evidence. This is particularly true in the context that it is now very easy for anyone to forge screen-shots of online postings.

### 3.5 Encrypted services

Some believe that if end-to-end encryption services that prevent security services from accessing material were banned or controlled, there would be less abusive behaviour online. This is not true, nor is it a good public policy.

Encryption is just mathematics, and it knows neither that its use is for ill or good. However, when you consider the extent to which encryption is being used – every website that uses `https` as part of its address encrypts the traffic between itself and its users, and that is nearly every website around the world – the good uses vastly outnumber the bad uses. If people are forced to use an encryption system that has been modified to make it easy for security services to gain access to the messages, it means that all the good, innocent uses of encryption are at risk. Recent news that Russian spies managed to infiltrate

[12] *Christchurch attack video footage and document has been banned in NZ – what this means for you* (https://www.classificationoffice.govt.nz/news/latest-news/christchurch-attacks-press-releases/#christchurch-attack-video-footage-and-document-has-been-banned-in-nz-what-this-means-for-you)

[13] Forensic Architecture, `https://forensic-architecture.org/`, is a research group that investigates alleged abuses of human rights using image and video records of events. To criminalise the sharing of such imagery and videos with no regard as to the purpose for the sharing plays directly into the hands of those who disregard victims' civil rights. Similarly, it's not correct to assume that police or intelligence services alone perform these types of investigations, so limiting permission to share to these organisations would not be sufficient.

the FBI[14], highlights how unreliable are assurances from security services that they can keep secrets such as the keys to all encryption safe from harm.

All it takes is one determined intruder, and all the good uses of encryption are put at risk in order to save money and effort on investigating illegal activities.

I have written a number of articles on this matter providing more details:

- *The value of encryption* (http://www.gibiris.org/eo-blog/posts/2015/03/12_the-value-of-encryption.html)
- *How can encryption be regulated* (http://www.gibiris.org/eo-blog/posts/2015/03/18_how-can-encryption-be-regulated.html)
- *You just can't stop people from using encryption, so stop trying* (http://www.gibiris.org/eo-blog/posts/2018/08/21_you-cant-stop-people-from-using-encryption.html)
- *Post-script on why you should stop trying to stop people from using encryption* (http://www.gibiris.org/eo-blog/posts/2018/08/22_stop-people-from-using-encryption-postscript.html)
- *Some questions for the "5 Eyes" countries on what they think they can do* (http://www.gibiris.org/eo-blog/posts/2018/09/04_some-questions-5-eyes-countries-what-can-they-do.html)

# 4 Answers to consultation questions

The following are some answers to the questions posed in the call for submissions.

## 4.1 Definition of communication in legislation

**Question 1** There are currently significant gaps in legislation with regard to harassment and newer, more modern forms of communication. Is there a need to expand the definition of 'communications' to include online and digital communications tools such as WhatsApp, Facebook, Snapchat, etc. when addressing crimes of bullying or harassment?

**Answer** Yes. However, it is important to consider the following:

- Not all such tools are as large and have such human and financial resources as the specific services referred to. Legislation that makes the assumption that such communication can take place only through services that are as large and wealthy as these will stand a very good chance of restricting or limiting competition in

[14] *Exclusive: Russia carried out a 'stunning' breach of FBI communications system, escalating the spy game on U.S. soil* (https://news.yahoo.com/exclusive-russia-carried-out-a-stunning-breach-of-fbi-communications-system-escalating-the-spy-game-on-us-soil-090024212.html) (Please note that to access this story the user has to agree to many hundreds of forms tracking or spend up to an hour examining those forms and disabling each one individually. It is recommended that this story be access using "Incognito" or "Private Browsing" mode in order to be protected against tracking).

these services' domains by imposing regulatory barriers of entry. I expand on this in the "Self-hosting" section of this submission.

- Legislation should focus not on the tool, but on the behaviour. In the main, therefore, it's the behaviour of those performing the bullying or abuse that should be targeted and not the "tool" used as the communications medium. I expand on this in the "User behaviour" section of this submission.

**Question 2** What lessons can be learned from models used in other jurisdictions such as the UK, New Zealand, Australia and other European countries where legislation is now in place to address these issues? How do we establish an appropriate model without compromising free speech?

**Answer** The incentives need to be present to ensure that the balance is managed correctly. Any legislation, such as *FOSTA-SESTA*[15] in the US, that seeks merely to punish web sites, will do more harm than good[16]. The incentive for US-based web site operators in this case is either **never** to host information for or by sex workers for fear of falling foul of the law, or to cease operations altogether. The result has been a human rights disaster, as sex workers, particularly women, are now at greater risk than before due to the failure of the law to consider the effect of a straight ban.

The recently-passed new EU Copyright Directive mandates the filtering of user uploads based on prior notice that such uploads **may** be infringing copyright and failure to implement this filtering is subject to severe penalties. However, the directive requires mere respect for users' freedom of speech with no penalties attaching to failing to do so. The incentive for the service operators here is to err on the side of suppressing material regardless of anyone's freedom of expression, as the consequences of keeping the material up could be catastrophic for the service operator and the consequences of infringing on someone's freedom of expression are non-existent.

The proposal in the UK to apply a duty of care to service operators is destined for failure, as a duty of care is a physical-world concept that has no suitable analogy in the context of internet services.

Ironically, the likely best regulatory approach is one that online services currently operate under in the US and to a large degree in Europe: intermediary liability protection. All these services maintain terms and conditions ("Community Rules", "Code of Conduct", etc.) and confirmed violations of these result in sanctions on the users, up to and including permanent exclusion from the service. However, where services aren't aware of violations, they are protected on the grounds that the behaviour that is objectionable is not that of the

[15] `https://en.wikipedia.org/wiki/Stop_Enabling_Sex_Traffickers_Act`

[16] Lura Chamberlain, FOSTA: A Hostile Law with a Human Cost, 87 Fordham L. Rev. 2171 (2019). Available at: `https://ir.lawnet.fordham.edu/flr/vol87/iss5/13`

service operator, but is of the user. In short, punish the user, not the service provider, unless – of course – the service provider is complicit.

**Question 3** How do we ensure that any legislation that is enacted is flexible enough to keep up with changing and advancing technologies, new apps and other online forums, including the more familiar social media sites?

**Answer** This is this submission's core concern. For legislation to focus on the technology, and not on the behaviour, to focus on the service operator and not on the real offender, runs real risks of damaging human rights of innocent parties, as well as stifling innovation and consolidating the market positions of the major operators

## 4.2 Harassment, stalking & other forms of online abuse

**Question 4** Online harassment can take the form of on-consensual taking and distribution of intimate images or videos, otherwise known as 'revenge porn', 'upskirting', 'downblousing' and other forms of sharing of imagery online without consent. What approaches are taken to addressing these issues in other jurisdictions?

**Answer** This submission is not offering any answer to this question.

**Question 5** New offences are proposed to cover these issues in Deputy Brendan Howlin's Private Members Bill on this subject. Is the creation of new offences necessary, or is existing legislation sufficient? Should other forms of image-sharing issues - such as exposure - also be addressed?

**Answer** This submission is not offering any answer to this question.

**Question 6** What kind of oversight and regulation of online service providers is possible/used in other jurisdictions? Currently, online providers are self regulated. Is a proactive, self-regulating approach from online companies to activities such as revenge porn and other forms of harassment preferable to the creation of more laws?

**Answer** If a measure of self-regulation to address these concerns is acceptable, then it would be necessary for public-perception reasons, to be clear on what that means. *Self-regulation* could mean either where each service operator manages matters of harassment and harmful communications according to their own rules and processes. This is currently how the large service providers we're most familiar with operate. However, *self-regulation* may also refer to regulation by a non-governmental industry-funded body, following the model of the press council or the advertising standards authority, where rules and processes are agreed among the operators as a set of standards, and where decisions of compliance to these are made by this body.

Aside from making this comment on the term, what is more important is getting the competing rights correctly balanced, rather than the model of regulation that asserts that balance.

**Question 7** Is any data provided by online service providers in relation to the reporting or prevalence of activities such as upskirting/revenge porn/cyberbullying and other online behaviour that can be used to develop and draft future legislation?

**Answer** Each of the major sites prepare what are called "Transparency Reports". However, many of these reports are constrained by rules laid out by (in particular) the so-called "Intelligence Community" of the United States. Thus these reports are not as transparent as they could be.

It should be a requirement for such services to issue a periodic report detailing the following statistics in each:

- The number of reported postings, broken down by nature of the complaint
- Number of reports that were appealed to the service, broken down by the nature of the complaint and the basis of appeal
- Number of appeals upheld, broken down by reason for appeal
- Number of appeals rejected, broken down by reason for rejection.
- Number of complaints/appeals that were appealed further to the regulator or courts system.

**Question 8** To what extent are An Garda Síochána equipped and resourced to deal with the issues arising from harmful online communications such as these?

**Answer** This submission is not offering any answer to this question.

**Question 9** Should 'cyberstalking' be treated as a separate offence to online harassment? What constitutes stalking-type behaviour online? Is there a need to legislative specifically for this activity?

**Answer** This submission is not offering any answer to this question.

**Question 10** Based on the findings of other jurisdictions such as in the UK, An Garda Síochána will require consistent training in order to maintain an appropriate level of knowledge with regard to indictable behaviours. Are resources available for this?

**Answer** This submission is not offering any answer to this question.

**Question 11** Fake accounts/troll accounts used to harass or target others with abuse – what measures can be taken in relation to these without effecting freedom of expression?

**Answer** The assumption that an account that isn't clearly associated with a personal identity is "fake" needs to be challenged. It is the *behaviour* of the account than needs to be considered. This is true of accounts that are associated with identifiable individuals as well as of pseudonymous accounts[17].

It should not be assumed that pseudonymous accounts are created in order for the users to escape legal consequences for criminal communications. There are many reasons for maintaining a pseudonymous presence online, some of which I have personally encountered being:

- To protect against a physically abusive family member
- To protect against an employer that monitors online activities
- To engage online in a manner that deals with prejudices (e.g. many respond to women differently than to men, to people of a different religion or skin colour than to those of the same religion or skin colour, etc.)
- To protect against action from their own governments whose laws are less respectful of civil rights as we would think Ireland's are.

It should not be assumed that a pseudonymous account has been created for reasons of abuse or harmful communication. In fact, there's good reason to assume that the significant majority of pseudonymous accounts operate for completely innocent reasons[18].

**Question 12** Do other jurisdictions have statutory measures to protect victim identities in cases of online harassment being released online posthearings, etc?

**Answer** This submission is not offering any answer to this question.

## 4.3 Harmful online behaviour and young people

**Question 13** How do we most appropriately regulate social media platforms to prevent cyberbullying and inappropriate sharing of personal images?

**Answer** I refer you to the details of this submission.

[17] A well-known Irish public figure who offers commentary on many aspects of society frequently posts messages on Twitter designed to elicit angry responses. I describe this person as "A master of the false equivalence". This is classic online trolling behaviour. Similarly, on the 18th September 2019, a prominent UK journalist tweeted personal details of a man who publicly challenged UK Prime Minister Boris Johnson regarding the state of the NHS. This act by the journalist was construed by many as deliberate trolling designed to inflict a measure of unofficial retribution on the man.

[18] facebook excepted. However, facebook's real-name policy is itself wrong, and does a great deal of damage to people who have good reasons for their names not to be associated with their online presences.

**Question 14** For young people who participate in such online behaviour as consensual image sharing, how can it be ensured that they are not inadvertently criminalised when legislation is enacted? What safeguards can be put in place?

**Answer** This submission is not offering any answer to this question.

**Question 15** Deputy Brendan Howlin's Private Members Bill provides that those under 17 should not be fined/imprisoned but put into relevant education or supports. Would these supports be part of the same educational supports offered to all young people/schools or would they be a separate entity? Are current supports being utilised? Are there sufficient resources to provide for such a provision when enacted?

**Answer** This submission is not offering any answer to this question.