Why Do Legislators Keep Failing Victims in Online Harms?

Andy Phippen[a]* and Emma Bond[b]

[a]*Bournemouth University, Poole, UK;* [b]*University of Suffolk, Ipswich, UK*

*aphippen1@bournemouth.ac.uk

Why Do Legislators Keep Failing Victims in Online Harms?

Keywords: online harms, online safety, harm reduction, image based abuse, prohibition.

Will Someone Please Think of the Children!

> Baroness Harding of Winscombe (Con)
> My Lords, it is an enormous privilege to follow so many powerful speeches. My second daughter was born in the year Facebook launched in the UK and Apple sold its first iPhone. Today she is 15; she has lived her whole life in a digitally enabled world. She has undoubtedly benefited from the great things that digital technology brings, but, throughout that life, she has had no meaningful legal protection from its harms.
>
> A number of noble Lords have referenced the extraordinarily moving and disturbing briefing that Ian Russell and his lawyer, Merry Varney, gave us on Monday. When I went home from that briefing, first, I hugged my two teenage girls really close, and then I talked to them about it. My 15 year-old daughter said, "Mum, of course, I know about Molly Russell and all the awful content there is on social media. Didn't you realise? When are all you adults going to realise what's going on and do something about it?" The Bill is important, because it is the beginning of us doing something about it.[1]

The above quote is drawn from a debate in the UK Parliament's House of Lords in early 2023, around the development of new legislation in order to ensure the population is protected from online harms. As an illustrative quote around the rhetoric of the debate, it shows the intentions of policy makers to both personalise the goals of

[1]https://hansard.parliament.uk/Lords/2023-02-01/debates/67BA25B1-DF5D-4B0A-9DA0-51246B0A8BD5/OnlineSafetyBill?highlight=harding%20online%20safety%20bill#contribution-FC570A74-ED27-4F25-88F4-D1FBE1A456F8

the legislation ("as a parent"), and place to protection of children at the forefront of its development ("we need to protect the children"). Given the current political attention on online harms and the legislation that will subsequently emerge, we will draw upon other examples from such debates throughout this article as we unpick and explore the question posed in this article - *Why Do Legislators Keep Failing Victims in Online Harms?*

In addressing this question, we will explore these debates in parallel with our own empirical work and reflect upon the legislative developments to tackle online harms in the UK over the last 15 years to understand how we have arrived with legislation that remains lacking in victim impact. We will raise fundamental concerns about a lack of victims' voice, a dearth of understanding about the nature of online harms, and an ideological obsession with legislating a particular stakeholder (online providers) while ignoring the responsibilities of others. Specifically, we will explore image-based abuse as a form of online harm that has attracted the attention of policy makers for a number of years, with some legislative success, while still failing to understand the needs of victims, particular minors. Specifically, we will explore the developments in law from 2015 to 2023, with a focus on section 33 of the Criminal Justice and Courts Act 2015, the landmark "revenge porn" legislation, its subsequent application and concerns, and the recently assented Domestic Abuse Act 2022, whose section 69 attempts to plug the holes that existed in the original legislation. Underpinning this discussion will be our view that legislators keep on getting this wrong because they fail to learn from history and do not understand that online harms should be tackled as a social harm, not a technological challenge. One of our fundamental concerns is that, given the digital nature of the nature of a lot of online

harms, the focus of legislation also lies with the digital technology, and policy makers often claim that online harms present "new dangers"[2]:

> The Secretary of State for Digital, Culture, Media and Sport
> (Ms Nadine Dorries)
> …In the past 20 years or so, it is fair to say that the internet has overwhelmingly been a force for good, for prosperity and for progress, but Members on both sides of the House will agree that, as technology advances at warp speed, so have the new dangers this progress presents to children and young people

However, we would argue that there have been other historical social policy efforts, with a focus upon prohibition, particularly the "war of drugs" which demonstrates similar rhetorical devices, that can be drawn upon, and learned from, in order to reframe these debates to be more victim centric and also drawn a wider stakeholder group.

History Repeating Itself

Since the mainstream adoption almost twenty years ago of what are sometimes referred to as "Web 2.0" technologies (O'Reilly, 2009), concerns have been raised regarding the potential for harm online (Livingstone et al., 2008). Using the UK as a case study, we argue that, even after all of this time, we still see little efficacy of legislation to protect victims from online abuse, which is certainly borne out in our own empirical work.

The UK provides us with a detailed case study given that, for the last twenty years, we have been immersed in both policy and practice around online safeguarding. During this time, we have conducted and published much research (for example

---

[2] https://hansard.parliament.uk/Commons/2022-04-19/debates/F88B42D3-BFC4-4612-B166-8D2C15FA3E4E/OnlineSafetyBill#contribution-6CBD6BCC-325E-4710-B8FB-9A4F82C732E3

Phippen 2009, Bond 2010, Bond 2013, Bond 2014, Phippen 2016, Phippen and Bond 2020, Bond and Phippen 2022) with most of this work being victim centric with a focus on developing policy arguments based upon their voices. And over this period there is a consistent response from the stakeholders (young people, adult victims of online abuse, safeguarding professionals, police, legislators, policy makers, etc.) – things are not getting better. We should stress that this current online harms policy cycle is certainly not the first one, arguably that started with the concerns of the Labour government in the UK in 2008 and the commissioning of the Byron Review (Byron, 2008). In all this time the rhetoric has remained the same – "we will protect citizens from online harms, we will eliminate online harms, we will hold those responsible to account". Yet the goal to "protect children and the vulnerable online"[3] seems to have consistently failed, given our conversations where young people will still say they will not disclose upset or harm for fear that stakeholders with responsibility for their safeguarding will "freak out" or "make things worse" (Phippen and Street, 2022).

We have, in this time, developed a stakeholder model for online harms based upon Bronfenbrenner's (1979) Ecology of Child Development, a well-established and widely used model for child development that can be developed to consider stakeholder responsibilities around online abuse. Bronfenbrenner's seminal work applied both nature and nurture perspectives to a child's development stating that their own biology

[3] We also see this rhetorical device used in much debate – for example: https://hansard.parliament.uk/Commons/2020-12-15/debates/1B8FD703-21A5-4E85-B888-FFCC5705D456/OnlineHarmsConsultation#contribution-D2B84BB2-E5A3-49E3-8110-634CF406C357

is central to their development, but interactions with other actors in their environment, such as family, community and society all play a part in development and an action in one of these actors will impact across the wider ecosystem of development. Therefore, we can conclude, in order to provide the most effective context for child development, we should not just look at the child, but its environment as well:

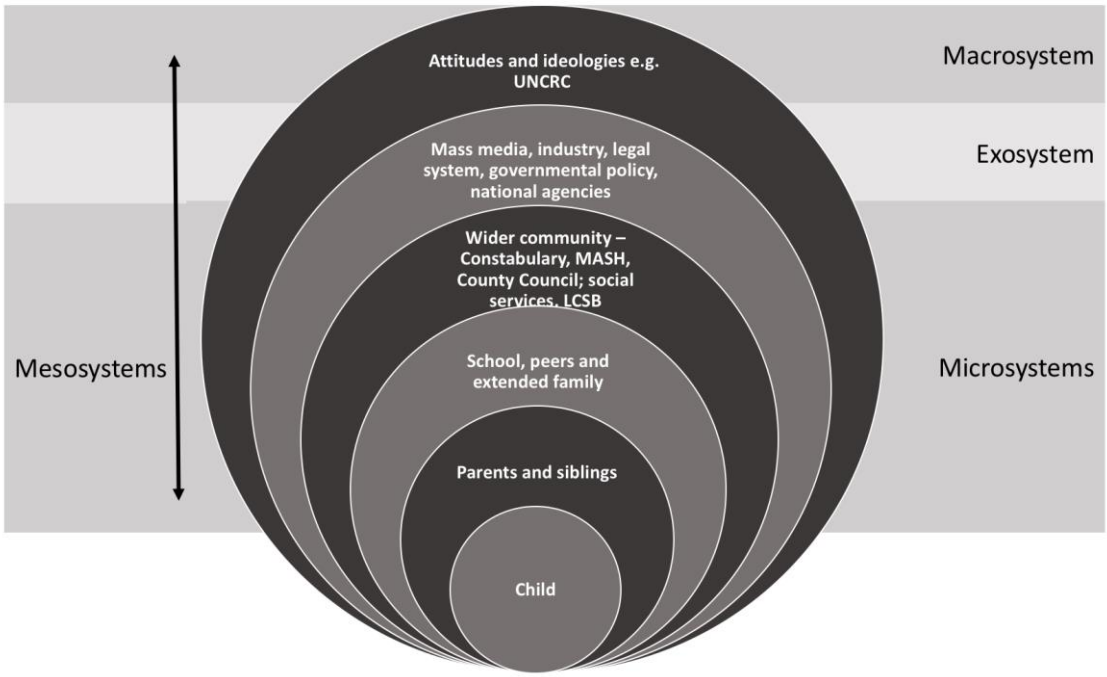

Figure 1 - An Online Safeguarding Ecosystem

The immediate spheres which influence a child's life and their landscapes of risk include their school teachers, peers, local law enforcement, social care and local authorities as well as everyday physical and virtual environments. All have statutory responsibilities for the welfare and safeguarding of the child both online and offline and, whilst industry does not sit within these microsystems, it exists in the broader exosystem that providers infrastructure for the child's online experiences and the views of other stakeholders within the microsystems.

The value of the model is that it shows the many different stakeholders in online safeguarding, and shows the importance of interactions (mesosystems) between them, as well as the distance a given stakeholder is from the student we wish to safeguard. Adopting a more holistic view of working with others to support young people in their online risk taking and decision making is far more effective, as stakeholders can bring their own expertise to the safeguarding role.

It is our view, having developed this model in consultation with young people and those with safeguarding responsibilities, that we need to move from believing we can prevent harms to understanding that knowing about risk and reducing the risk of harm are far more effective and also importantly more sustainable through the lifespan.

We are certainly not unique with this approach, and other scholars (for example, Ringrose et al., 2013, Setty 2019, Setty 2020) align their work with a strong qualitative approach and a focus upon representation of the victim, while calling for multi-stakeholder approaches to supporting victims. However, as we will explore below, we might, pessimistically, conclude that approaches that are underpinned in victim support, education, or multi-stakeholder approach and responsibility are often dismissed as too complex or "making things too difficult". If we were to reflect cynically upon some of the conversations, we have had with policy makers, these approaches do not fit in with political cycles or have sufficient political capital for the policy makers to engage with. Far better, it would seem, to shout at platform providers and tell them its their fault.

The Online Harms Policy Cycle

In April 2019 the UK Government released its *Online Harms* white paper (UK Government, 2019):

The government wants the UK to be the safest place in the world to go online, and the best place to start and grow a digital business. Given the prevalence of illegal and harmful content online, and the level of public concern about online harms, not just in the UK but worldwide, we believe that the digital economy urgently needs a new regulatory framework to improve our citizens' safety online.

Illegal and unacceptable content and activity is widespread online, and UK users are concerned about what they see and experience on the internet. The prevalence of the most serious illegal content and activity, which threatens our national security or the physical safety of children, is unacceptable. Online platforms can be a tool for abuse and bullying, and they can be used to undermine our democratic values and debate. The impact of harmful content and activity can be particularly damaging for children, and there are growing concerns about the potential impact on their mental health and wellbeing.

It continued:

This White Paper sets out a programme of action to tackle content or activity that harms individual users, particularly children, or threatens our way of life in the UK, either by undermining national security, or by undermining our shared rights, responsibilities and opportunities to foster integration.

There is currently a range of regulatory and voluntary initiatives aimed at addressing these problems, but these have not gone far or fast enough, or been consistent enough between different companies, to keep UK users safe online….

…The UK will be the first to do this, leading international efforts by setting a coherent, proportionate and effective approach that reflects our commitment to a free, open and secure internet.

As a world-leader in emerging technologies and innovative regulation, the UK is well placed to seize these opportunities. We want technology itself to be part of the solution, and we propose measures to boost the tech-safety sector in the UK, as well as measures to help users manage their safety online.

Perhaps the most telling comment from the opening pages of the white paper, however, comes from the Ministerial introduction, that stated the paper formed part of the '*UK's wider ambition to develop rules and norms for the internet*'.

Is it really the UK government's place to develop rules and norms for the internet as a whole? Of course, we would expect them to provide the legislation to manage behaviours that might be facilitated online that affect *their* citizens, but the intention to be the world leader in defining *norms* for a global network of interconnected devices smacks of ethnocentrism. We are minded to reflect upon previous efforts to adopt a technical focus for the regulation of global connected technologies. In 1996, John Perry Barlow published his Declaration of Cyberspace (Barlow 1996), stating:

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.

The declaration was written on the day the US Telecommunications Act 1996 (FFC, 1996) came into force. While the US government claimed this act would introduce great competition to the telecommunications infrastructure market, those who opposed it claimed it would consolidate power into the hands of a few major corporations (which turned out to be mostly true). *Internet Libertarians*, of which Barlow claimed to be among, wished for a free and neutral digital world and felt these early attempts to control online communications and place it in a competitive space, were doomed to fail. The declaration continued:

> Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions.

While we would perhaps distance ourselves from the view that *any* attempt to regulate technology is doomed to fail, this often-quoted statement is a useful tool with which to reflect upon the trials governments, with their geographical boundaries and extra-jurisdictional challenges, face if their legislative approach is to control the underlying technology or see the social solution for the reduction of harms being a technical one.

We are reminded of Ranum's Law (Muffat, 2016), a frequently quoted statement used by many in the technology sphere (mainly those pointing out flaws in legislative direction), attributed to the cybersecurity executive and researcher Marcus Ranum, which states:

> You don't solve social problems with software

During the time we have worked in this area, we have seen many attempts to regulate and control online behaviour through platform intervention and technical measure. These tend to follow in an approximate four to five year cycle. While the debates around the Online Safety Bill, its efficacy and whether it will "Make the UK the safest place to go online in the world", go on, those of us with longer memories can see it in a continuum of failed policy attempts to prevent harms.

The last large piece of "tech policy" was the Digital Economy Act, enacted in 2017 (UK Government, 2017), with its attempt to place age verification technologies onto pornography platforms to ensure children cannot access pornography. This piece of legislation was withdrawn in 2019, much to the shock of some politicians and media commentators.

Prior to that, in arguably the first major speech by a UK Prime Minister about online safety, David Cameron delivered a "call to action" in 2013[4] to ensure that children could not access pornography. In this case it was not the platforms who were targeted but the Internet Service Providers, who were mandated to implement "family friendly" filters on consumers' internet connections. If we are to measure the success of this technological intervention to ensure children are "safe" online, the most recent survey by the UK communications regulator, OFCOM exploring the attitudes of parents and children to media use (OFCOM, 2022) makes for illuminating reading. This states that a minority of parents (27%) have filters installed on all devices at home. The report goes on to state that 61% of parents say they have awareness of such tools but fail to implement these "potentially useful" (OFCOM's words) tools in the prevention of access in inappropriate content.

Should we conclude from these findings that parents in the UK do not care whether their children have access to "harmful" adult content? Or might it more reasonably be that they know these tools do not work, or have tried them and found them excessively restrictive and have chosen instead to focus on discussion and risk mitigation? In the same OFCOM report parents disclosed the most likely outcome for a child discussing upset that had occurred online was to talk to them about it (89%) rather than rely on technical intervention (25%).

Before Mr Cameron's attempts to protect children and the vulnerable from online harms, the last Labour government commissioned the Byron Review in 2008, whose report set out 38 wide ranging recommendation across various stakeholders in

[4] https://www.gov.uk/government/news/pm-hosts-internet-safety-summit

tackling online safety, including a self-regulation model for industry[5], that would "make the digital world a safe place for children". Very few of the Byron review recommendations which, to the report's credit, were aligned with a multi-stakeholder perspective, were ever implemented. With the change of government and lobbying pressure, the subsequent prime minister, instead, adopted an almost entirely provider focussed policy around stopping children accessing pornography which, as illustrated above, achieved little success.

Now, at the end of 2022, we await assent or quiet disappearance of the Online Safety Bill, we wonder whether this policy direction will ever be successful in its aim, or whether, when the next cycle of online safety policy commences, there will be any attempt to learn from history.

And we would not doubt the good intentions of policy makers in this space. There is clear intention to tackle the problem of online harms to meet both media and public concerns around the impact of harmful online content and conduct on society with, generally, a specific focus on the impact on young people. However, the prevalent view seems to adopt two key challenges:

(1) It is possible to stamp out these harms.
(2) Because it happens on digital technology, digital technology is the means by which harms should be prevented.

[5] https://learning.nspcc.org.uk/media/1045/byron-review-10-years-on-report.pdf

And it permeates from policy into practice. One of the leading providers of support around online safety in the UK is the UK Safer Internet Centre[6]. On its website it claims its mission is:

> Making the internet a great and safe place for children and young people

The UK Safer Internet Centre was (and arguably remains) part of the EU network of Safer Internet Centres established from 2004[7]. While the UK Safer Internet Centre's funding is no longer from the EU (it now receives funding from the Nominet Trust), its mission statement has remained consistent in all this time. And while it has unquestionably done great work over this period, in terms of awareness raising and educational resources, it has existed in some form for almost twenty years. And in this twenty-year period, the calls from young people with whom we have spoken remain the same:

- We want better education.
- We want to be able to disclose without risk of chastisement.
- We want the tools to be able to mitigate risk.

We are confident, reflecting upon our experiences over the last twenty years, that no victim or potential victim of online harms has ever told us that they want the government to "bring big tech billionaires to heel".

There is little evidence through this generational change, that this obsession with stopping/banning/eliminating online harms has been successful. And we frequently return to the question: If stopping online harms was straightforward, wouldn't we have done it by now?

---

[6] https://saferinternet.org.uk/about

[7] https://digital-strategy.ec.europa.eu/en/policies/safer-internet-day

The Safety Contradiction

> Michelle Donelan [8]
> We have to get this right… Children are at the very heart of this piece of legislation. Parents, teachers, siblings and carers will look carefully at today's proceedings, so for all those who are watching, let me be clear: not only have we kept every single protection for children intact, but we have worked with children's organisations and parents to create new measures to protect children. Platforms will still have to shield children and young people from both illegal content and a whole range of other harmful content, including pornography, violent content and so on. However, they will also face new duties on age limits. No longer will social media companies be able to claim to ban users under 13 while quietly turning a blind eye to the estimated 1.6 million children who use their sites under age. They will also need to publish summaries of their risk assessments relating to illegal content and child safety in order to ensure that there is greater transparency for parents, and to ensure that the voice of children is injected directly into the Bill, Ofcom will consult the Children's Commissioner in the development of codes of practice.

The above quotation is taken from the reintroduction of the Bill in 2022, after much stalling during the more turbulent days of the current government. Again, as with the opening quote in this article, the rhetoric is one of prevention, protection and even "shielding", all wrapped around a child protection narrative. We must, it seems, prevent children from being harmed if they go online. The rhetoric is subjective and, one might argue, somewhat frantic. If one explores the debates in depth (which are too numerous to be evidenced in detail in this article) we can see many examples of this almost hysterical panic in the need to tackle these social harms. We can illustrate again with a comment taken from the early 2023 House of Lords debate on the legislation:

---

[8] https://hansard.parliament.uk/Commons/2022-12-05/debates/10F81902-417B-4CE7-9B87-B50906663DB1/OnlineSafetyBill(Programme)(No4)?#contribution-A82F83F5-5BDA-4B24-86CD-032E83C33F53

Baroness Uddin [9]

(Non-Afl)

As co-chair of the APPG on the metaverse and web 3.0, working with stakeholders in this space, I recognise the power of innovative technology as a force for good. At the same time, as a social worker, I want to scream out loud its threat. If we do not address the gravity of harmful content that normalises children viewing extreme material on violent pornography, diet, sexual exploitation, self-harm and revenge porn that shapes their young minds, we will have abdicated our role as protector of standards. Statistics from the NSPCC, Barnardo's, Big Brother Watch and the Internet Watch Foundation, on unprecedented and worsening levels of online access to material on grooming, sexual abuse, self-harm, bulimia and millions of unfiltered pieces of content, make horrific reading.

It is no surprise, therefore, that we see elements of moral panics as defined in Cohen's (2002) seminal work which considered how media discourse can be used to vilify social subcultures and fire up social concern about things of which mainstream culture has little knowledge.

The discursive formulae Cohen adopted to represent moral panics is pertinent these discussions:

- *new* (hard to recognise, "creeping up on the moral horizon"), but also *old* (relating to traditions and fables);
- *damaging*, but also *warning signs* for real danger;

[9] https://hansard.parliament.uk/Lords/2023-02-01/debates/67BA25B1-DF5D-4B0A-9DA0-51246B0A8BD5/OnlineSafetyBill?#contribution-15B1B5CD-A0DA-4D06-90F6-B519D15B3D1E

- *transparent* (out in the open for everyone to see) but also *opaque*, requiring detailed explanation from "experts" to make people aware of the "real harm".

Our policy makers, it seems, have positioned themselves as saviours, even when victims are not asking for salvation, there are asking for support.

Policy in this particular area highlights a number of key issues related to the role of legislation in controlling access to content or managing online social behaviours:

(1) "Do something, anything!!"
(2) Implement legislation that might not be possible with the technology available.
(3) Rapidly implement legislation without understanding the broader social context.
(4) Use older legislation to tackle something for which it was never intended.
(5) Legislation have knock on effects that impact on the rights of those wishing to engage in legal behaviour online.
(6) The legislation fails to achieve what it set out to do.

Or, to put it another way – the Politician's Syllogism that originated in political satire (Chen, 2007):

> "We need to do something"
> "This is something"
> "Let's do this!"

We would argue that online harms policy has a rich history of "doing something" and that the root cause of these policy failures is an ideological one – they all aim to *eliminate* harm. While online harms, in part, are manifestations of social harms and the abuse levelled by individuals on fellow members of society. Yet the

safety contradiction takes the view that we can stop them. If the policy space has been repeating itself since 2008, at what point might we accept that the approach we have chosen is perhaps not the correct one?

We would suggest that perhaps the starting point of "safety" is not helpful. with the term online safety. Defined in the Cambridge Dictionary[10] as:

> A state in which or a place where you are safe and not in danger or at risk

It is important to remember that danger and risk though are different concepts. Beck (1992, 21) helpfully defines risk as:

> As a systematic way of dealing with hazards and insecurities induced and introduced by modernization itself. Risks, as opposed to older dangers, are consequences which relate to the threatening force of modernization and to its globalization of doubt.

Are we suggesting that we can achieve an online environment, comprising many billion individuals on a myriad of platforms, where all users are not at any risk or in any form danger?

By using rhetorical devices around safety, a word of much weight but little tangibility in the online space, we would argue that the goals of policy makers are doomed to fail and, furthermore, mean that policy directions fail to acknowledge the *potential* for harm when going online. Perhaps a more challenging, yet more realistic approach to tackling social harms would be to say that there are some risks that potentially arise in any online interaction, and we must align policy with a direction incorporates a wide stakeholder base that better informs every one of these risks and

---

[10] https://dictionary.cambridge.org/dictionary/english/safety

how they might be mitigated. However, presenting this alternative and, one might argue, more complex narrative to online harms debates there is a risk that you might be attacked for not supporting the politicians – "We want to protect the most vulnerable, don't you?".

Image Based Abuse as an Online Harm

> Geraint Davies [11]
> (Swansea West) (Lab/Co-op)
> Five years ago, I introduced a private Member's Bill that would have made it illegal for explicit private and sexual pictures to be shared online without consent. Subsequently, a ban on so-called revenge porn was introduced. Thousands of victims are now coming forward to the police yet only a handful of cases are going to court because victims cannot have anonymity and have to prove malicious intent. Will the Minister ensure this is criminalised and that these obstacles are not in place, so that victims can get their just deserts and criminals can be punished?
>
> Matt Warman
> The hon. Member is right. Whether it is sexting or revenge porn, far too much has happened since his private Member's Bill that has not been positive. Our proposed legislation will be one way of tackling a part of that, but other important complementary pieces of draft legislation, to be introduced via the Ministry of Justice and the Home Office, will close all the loopholes with regard to the kind of behaviour he mentions.

The above exchange happened in 2020, in the early stages of what would become the catch all solution of the Online Safety Bill. It was clear that the new legislation would be able to tackle any online harm, to address the challenges of previous pieces of legislation. However, the nature of the bill gives little room to

[11] https://hansard.parliament.uk/Commons/2020-02-13/debates/A5CF7D6C-ECF0-459E-AE73-6D810E794236/OnlineHarmsLegislation

consider peer on peer abuse resulting from the exchange of private images. Its focus almost entirely on a novel model for technology regulation, underpinned with a "duty of care", whereby legislators do not try to control the technology of itself, but place the responsibility for ensure the technology is "safe" in the hands of the providers. This duty of care is enforced with the establishment of a regulator, who will have powers to assess this duty and impose fines and potentially further prosecution should the companies be found lacking. The motivation of the bill, it seems, centres on the regulation of platforms, rather than supporting the end user/victim of abuse. It is difficult to see how a technical intervention by a platform might tackle the harms associated with the non-consensual exchange of intimate images. And simply saying "we will tell the platforms to stop this" fails to appreciate the nature of the harm.

We would argue that with image-based abuse there has been some success in the legislation, albeit for adult victims of the non-consensual exchange of intimate images (Phippen and Brennan, 2020). However, there is still much criticism (see Bond and Tyrell, 2021) about a failure of legislators, and the wider criminal justice system and safeguarding stakeholders, to focus on victims and understand the broader nature of threat. And there is little in the platform liability model that will better support victims. As Bond and Tyrell explore in their work, the failures relate to a lack of understanding of the legislation by police officers and prosecutors, and the severity of impact of such abuse on the victim (alongside the potential for further victim blaming).

While, certainly, there is some limitation in exploring the legislation in one jurisdiction, literature analysing other nations (for example, Yar and Drew, 2019) and Cole et al., 2020) show that similar approaches are adopted and we would stress that this article is making use of UK legislation to illustrate the nature of the legislature when trying to tackle online harms, rather than being held up as a unique approach to

online harms legislation, especially given the above quotation claims that the emergent legislation, which we reiterate focusses almost entirely on the practices of platforms in removing harms, will prevent this form of abuse.

Image based abuse is a particularly interesting case study if we are to approach with a victim centric lens, because it is so different for adults and young people. Entirely different legislation is applied and while there have been a few cases of the "revenge pornography" legislation being applied in cases involving minors, this is rarely the case. However, it is also interesting because it had legislation specifically developed to support victims of image-based abuse, yet the legislation is still viewed by many as being ineffective. And this relates to one specific form of online harm, whereas the Online Safety Bill claims to tackle all of them.

However, none of these pieces of legislation really considered the distress caused to the victim by the sharing of such private imagery. In the Shattering Lives report (McGlynn et al., 2019) the authors described a "social rupture" that occurred when someone becomes a victim of image-based abuse. The impact of the sharing affects all aspects of their lives – it is not something that can be shrugged off or ignored.

Citron and Franks (2014) had already elaborated on psychological impact, raising concerns around anxiety that can possibly lead to suicidal thoughts. They were clear that the harm that can arise from the non-consensual sharing of images should not be underestimated. Moreover, there can be further impacts such as concerns for personal safety, body image anxieties, long-term trust issues, and simply the anxiety of not known where images have been posted, whether further images will emerge, or how many people and who have seen them.

The growing concern around the fitness of the law to protect victims of this sort of abuse resulted in the new 2015 legislation, driven in part by an adjournment debate

by the Conservative MP Maria Miller[12]. The outcome of this and other debates was consensus that there was a need to develop legislation specific to image-based abuse and the non-consensual sharing of images.

Section 33 of the Criminal Justice and Courts Act 2015 (UK Government, 2015) was thus developed and came into force on 13 April 2015 creating a new criminal offence of disclosing private sexual photographs and films with intent to cause distress. Crucial to the offence are: (a) the lack of consent of the individual appearing in the photograph and film; and (b) the intent to cause that individual distress.

However, one fundamental criticism of the legislation, and the one that resulted in amendment of the legislation with Section 69 of the Domestic Abuse Act 2021 (UK Government, 2021a), was the lack of culpability in the event of threat to disclose. In order to be found guilty under the 2015 legislation, the abuser has to have *actually* disclosed the images to a third party, whether this be private individual or posting to an online platform. The failure to acknowledge the severity of threatening to sharing images raised concerns with the efficacy of the legislation, and the potential of the legislation to support victims of abuse. If we consider the nature of image-based abuse within scenarios of coercion and domestic abuse, the possession and threat to share is arguably more powerful than the actual act of disclosure.

"I have these intimate images and unless you do as I say" is potentially a more coercive threat than "I have disclosed intimate images and you should do as I say". Once the images and/or other materials have been shared, the abuser, arguably, has less power over the abuse.

---

[12]https://hansard.parliament.uk/commons/2014-06-19/debates/14061947000003/RevengePornography

Section 69 of the Domestic Abuse Act addresses this specific issue, adding to this definition to consider the harm caused by a threat to send an image as well as actual disclosure.

Since assent of the legislation, it has been applied and effective, to some degree, within England and Wales. Ministry of Justice Crime Reporting for the offence since 2017 is detailed in table 1:

Table 1 - Ministry of Justice statistics on s33 of the Criminal Justice and Courts Act 2015.

	Year ending June 2018	*Year ending June 2019*	*Year ending June 2020*	*Year ending June 2021*	*Year ending June 2022*
Proceeded against	*267*	*215*	*138*	*222*	*267*
Convicted	*213*	*182*	*131*	*211*	*236*
Sentenced	*209*	*184*	*138*	*215*	*230*

We can see from this data that the legislation has been applied many times, and results in a high level of conviction. This could be a good thing. Once entered into the criminal justice system, few will be dismissed. What is less clear from this data, however, is the proportion of complaints that result in proceedings or conviction. Research by the Revenge Porn Helpline[13], a national service to support victims of image-based abuse, have published research (Revenge Porn Helpline, 2022) detailing the number of cases they deal with per year since its establishment in 2015:

Table 2 - Call numbers for the Revenge Porn Helpline

[13] http://www.revengepornhelpline.org.uk/

2015	2016	2017	2018	2019	2020	2021
521	708	1094	1300	1680	3146	4406

While direct comparisons cannot be made, given cases are likely to have increased due to an increase in awareness of the service over time, we can see that while there are clearly more people disclosing abuse as a result of image-based abuse, the number of prosecutions in England and Wales does not reflect this increase. This would suggest to us that the number of adult victims of image-based abuse in the UK is far higher than those who achieve any success in prosecuting their abuser. In discussions with the Revenge Porn helpline, there are some suggestions regarding why this might be the case.

In discussions with the Revenge Porn Helpline, while threat is a consistent element of abuse brought up by their clients, the issue of *intent* is one that presents more challenges to get the police or Crown Prosecution Service to take the abuse seriously and move to prosecute. The legislation is clear that intent to cause distress must be demonstrated:

Subsection 8 clarifies this is:

> A person charged with an offence under this section is not to be taken to have disclosed a photograph or film with the intention of causing distress merely because that was a natural and probable consequence of the disclosure.

This is further underlined with guidance from the Crown Prosecution Service (2017):

> A person will only be guilty of the offence if the reason for disclosing the photograph, or one of reasons, is to cause distress to a person depicted in the photograph or film.

And the College of Policing (2015) states:

> For the offence to be committed, the disclosure must take place without the consent of at least one of those featured in the disclosed picture and with the intention of causing that person distress

While the Domestic Abuse Act 2021 (iBid) updates subsection 8, it does so simply to incorporate threat:

> A person charged with an offence under this section is not to be taken to have intended to cause distress by disclosing, or threatening to disclose, a photograph or film merely because that was a natural and probable consequence of the disclosure or threat.

Intent still presents challenges to moving to charge or prosecute with these types of offences and provides an easy defence for an abuser. Unless intent can be proven it is unlike the CPS will proceed. This is certainly the experience of many of the clients supported by the Revenge Porn Helpline. The other issue is that of victim anonymity. The Sexual Offences (Amendment) Act 1992 (UK Government, 1992) defines several sexual crimes which grant the victim anonymity during court proceedings. At present image-based abuse remains defined as a communications crime, as confirmed in 2016 by the then Minister for Preventing Abuse, Exploitation and Crime. While orders have been made in individual cases, campaigners argue that the prospect of being named in the courts is a significant barrier for many victims to come forward. In June 2019, it was announced that the Law Commission would review anonymity for victims of image-based abuse[14] although this has yet to be acted upon and from a victim centric perspective, as evidenced by those who work at the Revenge Porn Helpline, they are

[14] https://www.gov.uk/government/news/law-around-non-consensual-taking-making-and-sharing-of-sexual-images-to-be-reviewed

very clear that anonymity is needed if we are to get more victims making reports to the police and receiving effective support during the criminal justice process.

While there is certainly evidence that the law has been successfully applied, and provides some level of protection for victims, it is perhaps not the policy success claimed by the legislators. However, it is a progressive outcome compared to the legal situation for minors faced with abuse following the non-consensual sharing of intimate images.

Just Say No

> Laura Farris[15]
> (Newbury) (Con)
> …We have produced, for instance, the Domestic Abuse Act 2021, which dealt with revenge porn, whether threatened or actual and whether genuine or fake, and with coercive control. Many Members recognise what was achieved by all our work a couple of years ago…. I should like them to explain to the House how they think the Bill will capture the issue of sexting, if, indeed, it will capture that issue at all.
>
> As the Minister will know, sexting means the exchanging of intimate images by, typically, children, sometimes on a nominally consensual basis. Everything I have read about it seems to say, "Yes, prima facie this is an unlawful act, but no, we do not seek to criminalise children, because we recognise that they make errors of judgment." However, while I agree that it may be proportionate not to criminalise children for doing this, it remains the case that when an image is sent with the nominal consent of the child—it is nearly always a girl—it is often a product of duress, the image is often circulated much more widely than the recipient, and that often has devastating personal consequences for the young girl involved.

---

[15] https://hansard.parliament.uk/Commons/2022-12-05/debates/E155684B-DEB0-43B4-BC76-BF53FEE8086A/OnlineSafetyBill? contribution-DD9DD3B0-3FE4-4488-ACE0-2465E64204CC

In the previous section we have briefly explored the development of legislation around a specific online harm – revenge pornography and the challenges in developing the law so that it is victim centric, highlighting specifically some challenges along the way around understanding the nature of the harm and how it should be tackled. And, while stakeholders with whom we work would still claim that it is still not hugely effective because, firstly, it fails to fully recognise the impact on victims, and that the ecosystem around the criminal justice system is neither aware of the extent of the harm.

However, if we should stress again that this legislation is specifically intended to support adult victims, and if we consider exactly the same act carried out by a minor, we end up in a particularly problematic legislative and policy mire, both in terms of the law itself, and also the attitude of those in power around willingness to support victims who will be as severely harmed (perhaps more so given the attitude of many who have safeguarding responsibilities for them) by the non-consensual sharing of an intimate image as an adult. The above quote, taken from the 5th December 2022 debate on the Online Safety Bill, highlights this difference in attitudes. Firstly, congratulating themselves for the legislation that has "dealt" with revenge pornography, and then concerns about the legal problems around similar for young people. However, the discourse here is not "we need to adapt the law to provide equal protects for minors who are victims of image-based abuse", it is instead "we need to stop young people doing this". The comment "we recognise that they make errors of judgment" is particularly telling and immersed in victim blaming culture.

Put simply, an eighteen year old victim of image based abuse, whose images are non-consensually shared with others, if protected in law and their abuser, potentially, could end up with a custodial sentence for doing so. If a seventeen year old is in exactly

the same situation, there is a possibility they might themselves be prosecuted for the manufacture and distribution of indecent images of a minor.

The legislation that is applied to teen sexting is old and developed to tackle an entirely different social harm. The Protection of Children Act 1978 (UK Government, 1978), was introduced as a private members bill with by Cyril Townsend MP. The title of the bill makes it clear this piece of legislation is intended to protect children, in the case of the bill from the exploitation of children in the production of pornography by adult abusers. In its introduction to the House of Commons, Mr Townsend stated:

> We acted to prevent abuse of little children as chimney sweeps and in the factories. We acted to prevent their abuse in dark satanic mills and deep down in the mines. Shall we act today to prevent their abuse in child pornography? [16]

Clearly, the intention is to protect children from exploitation. While the debates around the bill were long and detailed (explored in more detail in Phippen and Brennan, 2020) at no point in the debates was it suggested that this might be something enacted upon a minor from another minor or that the subject of the image was also the taker and distributor of the image.

Of course, in the late 1970s there is no reason to suggest anyone entertained the idea that in the future technology would be sufficiently advanced for an individual to take an intimate image of themselves and distribute it to peers using mass communication networks. The legislation was developed to prevent child exploitation,

---

[16] https://hansard.parliament.uk//Commons/1978-02-10/debates/d8d6a02b-8dab-4cde-8f05-3cbb1326f710/ProtectionOfChildrenBill#contribution-83f95c97-cc42-4eb5-b475-ebb2905662ef

yet ended up being used to revictimise younger victims of image-based abuse in a manner for which it was never intended.

Nevertheless, that is how the law has been applied, alongside educational messages around "don't send nudes, its illegal", without ever exploring the law and its failure to keep up with norms in modern relationships. And, because the law decrees, those wishing to address this particular social harm has an easy platform to say "just say no", rather than calling for changes to the law to ensure if the taker and send of the image is a minor and also the sole subject of the image, it cannot be considered a crime.

Alongside the application of this legislation, education messages developed around the legalities of these acts centred on blame and legality. "Don't send nudes", young people were told in assemblies and pastoral education lessons, "because its illegal". This has been consistent for twenty years, and we see the impact of these education messages on adult victims of image-based abuse, where the Revenge Porn helpline regularly tells us that victims who content them will say "I know it's my fault, I should never have sent the images in the first place".

Such was the concern of the application of this law to these new acts, acknowledged in 2016, that the police issued guidance[17] that allowed police forces, if called to an incident of intimate image sharing, to record it as an "Outcome 21" – essential, "this is not in the public interest to proceed, no further action taking place". This, we were told, was the solution to this out-of-date legislation. However, the guidance did still say such a recording could be return in some cases in a criminal records check and have an impact on a young person's future life course. And, as we

---

17 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/578979/GD8_-_Sexting_Guidance.pdf

have discovered (Phippen and Bond, 2020) Outcome 21s were being applied in different regions in different measures, and arrests of minors were also taking place in variable amounts.

Data from Ministry of Justice (iBid) highlighted that the law was still being applied to proceed against and prosecute minors:

Table 3 - Prosecutions of minors against Section 1 of the Protection of Children Act 1978 (2008-2022)

	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22
Proceeded against	39	41	41	40	34	40	50	56	61	55	45	42	43	59	53
Convicted	33	33	36	37	26	30	39	48	56	39	41	32	36	49	47
Sentenced	33	33	36	36	27	30	39	49	54	41	41	32	37	48	47

As we have discussed above, the prohibitive mindset extends into the education curriculum. While young people say they want a curriculum that informs them of the risks, tells them how these might be mitigated and where they might gain support for resolving any risks or harms, the focus of the current curriculum [ref] still resides with legislative messages and prohibition. In the current national curriculum for England, the only reference to sexting (the exchange of intimate images between peers) in the core specification lies in the “legal provisions” section, stating pupils should be made aware of relevant legislation when relevant topics are taught. Or, in other words, “they need to be told it is illegal”.

Of course, from a victim centric perspective the outcome from this is appalling and results in young people unwilling to disclose harm (for example, in the event of non-consensual sharing) or, if they do disclose, not receiving any support in rectifying the issues they are facing. A simple random sample of disclosures from Everyone’s Invited, a website where child victims of sexual harassment and abuse in schools

anonymously disclosed their experiences[18], easily found many cases of young people talking about these prohibitive messages and lack of support, including:

- Is it because it is easier to tell a child not to do it and make use of the law to scare them, rather than understanding the nuance and context around the acts of exchanging images and the relative impact based upon these factors?
- A young person who had intimate images shared non-consensually at the age of 13, who still suffers anxiety issues at the age of 21 as a result. The victim states that she blames herself.
- A young person pressured into sending nudes at the age of 12, who did so because she thought "that's how dating is these days".
- A young person who, after a sexual encounter with a peer, with the peer then claiming he'd taken images non-consensually and shared them with his friends. When she was sent the images, they were not of her, but when she disclosed the abuse to a teacher, instead of support they received a lecture on the dangers and legalities of sharing nudes.

These disclosures reflect the conversations we have had with young people over many years. When asked who they would disclose to if someone had non-consensually shared images of them, most said there was no way they would speak to a teacher or parent, this would result in being told off or far worse. Young people told us of situations experienced by peers where they found themselves in the headteachers office, with police and parents present, going through their phone and revictimizing them

[18] https://www.everyonesinvited.uk.

further by exposing their intimate images to a wider audience. Far better, and less "risky", we were told, to talk it through with peers.

Returning to the debate contribution by Ms Farris, the prohibitive mentality is demonstrated once more with a further comment:

> Laura Farris[19]
> (Newbury) (Con)
> … All the main internet providers now have technology that can identify a nude image. It would be possible to require them to prevent nude images from being shared when, because of extended age-verification abilities, they know that the user is a child… I should like them to address that specific issue of sexting rather than letting it fall by the wayside as something separate, or outside the ambit of the Bill.

Regardless of the technical inaccuracies of Ms Farris' statement, it is useful in returning us to the starting point of this article – that there is a belief in government that it is the role of platforms to prevent online harms to victims, no one else. There are no calls in the debates for improved education, or better training for teachers, the wider children's workforce, police or prosecutors. Instead, all online harms, it seems, can and should be stopped by the platforms upon which harms take place, or they could become criminally liable.

Harm Reduction, not Prohibition

The frustration for scholars who work closely around victims' voice, and who have spent a long time immersed in this field, is that, as we have already illustrated,

---

[19] https://hansard.parliament.uk/Commons/2022-12-05/debates/E155684B-DEB0-43B4-BC76-BF53FEE8086A/OnlineSafetyBill? contribution-DD9DD3B0-3FE4-4488-ACE0-2465E64204CC

there is an ideological obsession with prohibition and the belief that online harms are something that can be stopped, rather than mitigated. This is simply wrong. No amount of technology will prevent something that is, generally, caused *by* someone *to* someone. While technology can provide tools to manage online relationships and block and report abusers, they will never be able to proactively identify all harms, while allowing freedom of expression on online platforms.

There is also, as also demonstrated, a complete lack of understanding about past failed policy positions that have adopted this mindset, given the one particular aspect of online harms – stopping young people accessing pornographic content – has been a policy obsession for well over ten years yet, as young people tell us, they still access this sort of content. They also tell us that they do believe pornography has the potential to be harmful in developing unrealistic expectations, performance anxieties and body image issues and they need progressive educational approaches and safe spaces in order to be able to discuss these things. However, such progressive approaches seem to be missing from the Online Safety Bill debates.

In this article so far, we have presented an argument for the failure of policy and law that adopts a prohibitive approach to tackling one form of social harm – harms that happen online. We have, over the years, been frequently told by policy makers and politicians, that "the trouble with tech law is keeping up with the technology", which is why it is so difficult to achieve effective legislation. Yet we still see, as illustrated in the debate quotes presented in this article, that this does not stop them returning to the same position again and again – "we must stop online harms".

Fundamental to all these points is a prohibitive mindset where other areas of social harm have also been tackled in the past and, arguably, been extremely ineffective. The closest parallels, we would suggest, are with drugs policies of the 90s which aimed

to prevent drug use rather than understand the social context in which drug taking places and how "harm reduction" approaches that centre on evidence-based policy (Wood et al., 2010) can result in far more effective policy. We refer to the long "War on Drugs", and more specifically the Misuse of Drugs Act 1971 (UK Government 1971). In making use of debates to illustrate similar mindset, we can see the same calls and approaches by politicians when tackling the social harms associated with drug use and addiction. While there are some differences between drug harms and online harms, specifically around the drugs industry compared to the online harms ecosystem, it is still a useful comparator when considering prohibition ideology and there is much we can learn from, given, at least in part, the failings of prohibitive drug policy are acknowledged and there is evidence to show the value in more progressive approaches.

The parallels in debates between the introduction of the Misuse of Drugs Bill and the Online Safety Bill are interesting and certainly underscore the rhetorical devices used to argue for the need for these prohibitive legislations. In the introduction of the Misuse of Drugs act, Mr William Deedes MP, stated:

> (Mr William Deedes)[20]
> This Bill is mainly about young children, or it should be, and the unnerving thing about this epidemic is the way, certainly in the United States, in which the age of infection creeps downwards.
> Differs because the MODA 1971 doesn't focus entirely on one stakeholder.
> However, the prohibitive nature of the legislation is directly comparable. These are both acts that intend to prevent a social "harm" from occurring – either the consumption and distribution of illegal drugs and the subsequent anti-social acts

[20] https://hansard.parliament.uk/Commons/1970-03-25/debates/f91449c8-2f64-4b79-9bfc-0aa5f0c72908/MisuseOfDrugsBill#

> that occur as a result of drug consumption, or the consumption and distribution of harmful online content and prevention of abusive behaviours.

In other words, drugs are harmful, and we need to protect society, especially children and young people. Using similar rhetorical devices that align with the moral panics identified by Cohen (iBid.) the argument is immediately positioned as "If you care about children, you should support this legislation".

Furthermore, in the Misuse of Drugs Bill debate it was acknowledged that the evidence base was not sufficiently developed. Nevertheless, it was crucial a prohibitive approach was used. Far better, it would seem to prevent use than understand risk and harm in more detail:

> (Mr James Callagan)[21]
> But, at least, while we in this generation are searching for the causes of drug taking, let us not be responsible for any weakening in our attempts to stamp out what is at present a dreadful scourge. We know too little, even about the so-called benign drugs, to take any risks. As for the rest, their immediate and visible consequences are too dreadful to behold.

> (Mr. William Deedes)[22]

[21] https://hansard.parliament.uk/Commons/1970-03-25/debates/f91449c8-2f64-4b79-9bfc-0aa5f0c72908/MisuseOfDrugsBill#

[22] https://hansard.parliament.uk/Commons/1970-03-25/debates/f91449c8-2f64-4b79-9bfc-0aa5f0c72908/MisuseOfDrugsBill#

> We do not know what the psychological long-term effects are. Until we know, we must make it clear to the young that we do not know and that we maintain prohibition.

And a similar viewpoint was articulated by the then Secretary of State about online harms in 2022:

> (Mrs Nadine Dorries[23])
> Remember: we have been debating these issues for years. They were the subject of one of my first meetings in this place in 2005. During that time, things have got worse, not better. If we choose the path of inaction, it will be on us to explain to our constituents why we did nothing to protect their children from preventable risks, such as grooming, pornography, suicide content or cyber-bullying.

While we would question why, given Ms Dorries is keen to highlight that online harms policy, particularly prohibitive approaches, no one is suggesting maybe a change of path, it is interesting to note that, once again, many years later, our legislators are essentially saying "we do not understand this, so let's stop it".

The history of the "war on drugs" (while the phrase was coined, coincidentally in 1971, it arguably commenced in post prohibition USA with the establishment of the Federal Bureau of Narcotics in 1930) clearly shows a similar prohibitive mindset that criminalises users and attempts to deliver simple messages about stopping harms occurring by preventing the act of drug taking.

As can be seen from the timing of the introduction of the Misuse of Drug Act, these prohibitive approaches in drugs policy have been around for far longer than prohibitive online harms policy. More recently, however, there has been a large

---

[23] https://hansard.parliament.uk/commons/2022-04-19/debates/F88B42D3-BFC4-4612-B166-8D2C15FA3E4E/OnlineSafetyBill#

consensus around the need to move aware from prohibitive approaches to understand the motivations of users, the multi-facetted nature of drug use, and evidence lead policy categorising harms, leading to the Vienna Declaration (Wood et al., 2010), published in the Lancet by leading drug scientists in 2010, and also impacting away from academic literature in texts such as Johann Hari's (2015) Chasing the Scream.

In some democracies we have seen far more progressive drugs policy that looks very different to these prohibitive views. For example, the decriminalisation of all drug use in Portugal (Greenwald, 2009), alongside centres where people can safely take drugs, has not led to what some predicted would be massive increases in drugs use and overdose. Within the US, where some states have been even more progressive and built markets around the sale of some previously illegal drugs has, similarly, not resulted in increases in addiction or antisocial behaviour (Pardo, 2014). Famously, John Hickenlooper, the Governor of Colorado, one of the states that legalised the sale of cannabis, was quoted as stating in a speech prior to the introduction of the more progressive drugs legislation:

> Let's face it, the War on Drugs was a disaster. It may be well intentioned ... but it sent millions of kids to prison, gave them felonies often times when they had no violent crimes ... I was against this, but I can see why so many people supported it.

This is a particularly telling comment compared to Ms Farris' comments around the criminalisation of children for sharing intimate images, and the evidence that shows the law is still being used in this way.

Within the drugs policy area, more these progressive concepts have been developed, and the resultant programmes of intervention that have resulted from these more rights and justice-based approaches, are referred to as *harm reduction*. Harm reduction, in the drugs policy world, refers to policies and approaches that aim to

minimise not just health, but social and legal impacts of drug use, focussing on supporting users in an informed manner that allows them to make more positive choices and mitigate the risks associated with the taking of illicit drugs.

Four basic assumptions central to harm reduction have been defined as (Marlatt, 1996):

> (a) harm reduction is a public health alternative to the moral/criminal and disease models of drug use and addiction;
> (b) it recognizes abstinence as an ideal outcome but accepts alternatives that reduce harm;
> (c) it has emerged primarily as a "bottom-up" approach based on addict advocacy, rather than a "top down" policy established by addiction professionals;
> (d) it promotes low threshold access to services as an alternative to traditional high threshold approaches.

And the Harm Reduction Coalition in the US, defines eight Principles of Harm Reduction[24], that can be summarised as:

- Accept drug use as part of our world and we should work to minimize harmful effects rather than just condemn them.
- Understand that drug use is complex and multi-faceted and harms occur on a continuum
- Quality of life is more important than prohibition in successful intervention and policies
- Adopt a non-judgemental, non-coercive provision of services and resources to drug users and the communities in which they live.
- Users' voice should be a central part in the creative of programmes and policies designed to serve them
- The primary agent of a reduction in drug harms are from informed users
- Recognise the complex social factors that impact upon drug use and drug related harm

[24] https://harmreduction.org/about-us/principles-of-harm-reduction/

- Does not minimize or ignore the real and tragic harm and danger that can be associated with drug use

It is extremely straightforward to transpose these principles to the world of online harms – the adoption of a risk mitigation approach should be chosen over a prohibitive approach, and victims should not be met with victim blaming discourse. Risk mitigation is best address through education and information, and harms are complex relating to a wide range of social factors. Most importantly, do not view a progressive approach as one what minimises the harm caused by online abuse. However, it does not start with the unobtainable "we will stop this". Related back to our stakeholder model in figure 1, we can, once again, see how these principles work most effectively with a multi-stakeholder approach, rather than focusing prohibition on the delivery platforms.

While, compared to the duration of the War on Drugs and its failures, harm reduction approaches are still in their infancy, there is still an evidence base to show that adopting a multi-facetted, non-judgemental, evidence-based approach to tackling drug harms has been, in several locations, extremely successful. At worst it has not resulted in the predicted massive increases in social harms and at best provides better outcomes for drug users and the communities around them.

- Effective, progressive education delivered by those who understand the subject.
- Non-judgement and supportive responses to disclosures and support to mitigate risk.
- Policies and legislation that supports victims rather than criminalising them.
- Tools and responses from platforms which mean when they report something they can see what happens and they feel they have been listened to.

With its focus on a single stakeholder, the Online Safety Bill does nothing to embrace this approach. When we couple this with a political unwillingness to even tackle the clearly evidenced and well discussed failures of existing legislation (such as the sharing of intimate images by minors) and the prohibitive educational narrative around which so closely echoes of messages in drugs education in the 1980s and 1990s we still, almost fifteen years since the Byron Review called for a multistakeholder approach to tackling online harms, still have a just say no mindset. Returning to our opening question of: *Why do legislators keep failing victims of online harms?*

It is, if we reflect upon the quality of the debates and the evidence from policy outcomes, obvious. It is because we keep on doing the same thing, with different, but similar, voices saying it.

And while the approach may be somewhat untested in tackling online harms (although some elements of the online harms literature has called for multi- rather than single-stakeholder responses and progressive education for many years), it is at least thoroughly tested in another area of social harm. And harm reduction drugs policy is informed by an evidence base that says providing honest information about risks and how to mitigate those risks helps more people keep themselves safe than simple prevention approaches (Werch & Owen, 2002). While this might seem too progressive, fanciful and untested, what we are very clear about is the current approaches are not working, so we need to try something different. And the Online Safety Bill is not what we need.

We need to acknowledge that prohibition doesn't work before we can move toward more progressive policy approaches. However, this is not to say that the wider stakeholder group could not adopt more effective harm reduction approaches despite the policy makers.

We have often been faced with criticism from policy makers that we are always being critical, and we should be more supportive of their proposed approaches. There is a suggestion that we do not see providers as part of the solution and would not trust any technical intervention. This is not true. We are opposed to technical intervention that will not work and has the potential to impact negatively upon victims' rights. However, there are solutions that do work within a harm reduction framework.

The StopNCII platform[25] whch is a joint project between Meta and the Revenge Porn Helpline in the UK and makes use of a technology called image hashing to allow a victim to provide platforms and service providers with a unique identifier for their images, without having to share actual images with the platforms. The technology that underpins the service is well established in child protection, but for a different purpose.

The Internet Watch Foundation[26] has proactive powers to search online for illegal images of children. Once images have been identified as child abuse or exploitation material the image will be processed using Microsoft's PhotoDNA algorithms[27], which applies an algorithm to image data to produce a unique "fingerprint" for that image. For the IWF hash list, once the image has been identified and hashed using the Microsoft service, the hash will be stored. Therefore, a service provider can make use of the hashlist to process images it is accessing. It can then run the same PhotoDNA algorithm on any images it indexes, and if the hash matches, the platform knows, because it is in the IWF hash list, which means it has already been analysed by a human moderator and classified as illegal. Again, the "recognition"

---

[25] See https://stopncii.org/?lang=en-gb [Accessed February 2023]

[26] See https://www.iwf.org.uk/ [Accessed February 2023]

[27] See https://news.microsoft.com/2009/12/15/new-technology-fights-child-porn-by-tracking-its-photodna/#sm.0001mpmupctevct7pjn11vtwrw6xj [Accessed February 2023]

technology is very straightforward and easy to achieve – if the hash of the candidate image matches one in the hash list, it will be considered illegal and, at the least, blocked. This is technology that is well established, simple, and effective. Yet seems to be ignored in favour of more high profile, and less stable and effective solutions, in a lot of the online harms discourse.

With the StopNCII approach, a victim of image-based abuse can apply the hashing technology on their own device to their images (which they either know or hear have been non consensually shared). They can then upload their hashes to the Revenge Porn Helpline service, who will then distribute to service providers. Therefore, if someone attempts to non-consensually share that image on a platform that uses the service, the posting will be blocked. Most powerfully, perhaps, is that the victim does not have to show their images to anyone, they are empowered to hash the images themselves and need share only the hashes.

This is a great example of stakeholders working together – technology that works is used by platforms, and a civil society service provides the contact point for victims. Until recently this service was, however, only available to adults. However, at the time of writing (January 2023), the National Centre for Missing and Exploited Children in the US (NCMEC) have announced their Take It Down service[28], which applies the same technology on a service for young people. From a technical perspective, this is the first service of its kind that tries to empower young people with technology, rather than simply telling them what they have done is wrong, and it is an excellent example of using technology within a harm reduction approach. There is no need for the young person to show the images to anyone or even to disclose that they

[28] See https://takeitdown.ncmec.org/ [Accessed January 2023]

have taken them. In the same way as an adult victim would, they can take agency over the situation and ownership over their content, and ensure those who are threatening to share, or have shared, will be unsuccessful. Far more empowering, we would suggest, than simply telling them “Once its online its always online” or “it’s your fault for taking the images”.

Why Do Legislators Keep Failing Victims of Online Harms?

In conclusion, we return to the question posed in this article. We have explored these issues in detail in this article but would summarise as:

- Heroic rhetoric and the intention to save from harm means that any new policy starts with a goal that is unachievable. Far better, we would suggest, to adopt a risk mitigation and victim support approach than the utopian “safety” metaphor
- Failing to understand a multi stakeholder perspective and the potential of technology to tackle social harms, and instead prioritising demands on an industry that undoubtedly have a role to play, but not the solution.
- Prohibitionist approaches, particularly relating to supporting victims who are minors, risk revictimization and do not provide an environment for disclosure and support. A victim of any age needs help and support, not judgement.
- A failure to appreciate harm reduction approaches to tackle social harms, and a lack understanding of the evidence base, and the need for an evidence base, to inform policy decision.

While there might be some suggestion that harm reduction is untested related to online harms, and we would agree that there is a new to evaluate new initiatives adopting these sort of approaches. However, we have got considerable evidence that prohibitive approaches do not work. And failing to acknowledge this, and learn from previous

policy failures, means we will remain locked in this prohibitive policy cycle, regardless of government, and will continue to fail to meet the needs of victims.

References

Barlow, John P. (1996) Declaration of Independence for Cyberspace available from https://www.eff.org/cyberspace-independence

Beck, U. (1992) *Risk Society Towards a New Modernity*. London: Sage.

Bond, E. (2010) 'The mobile phone = bike shed? Children, sex and mobile phones' in *New Media & Society* Vol. 13 no. 4 pp. 587-604

Bond, E. (2013) 'Mobile phones, risk and responsibility: Understanding children's perceptions' in CyberPsychology: *Journal of Psychosocial Research on Cyberspace*

Bond, E. (2014) *Childhood, Mobile Technologies and Everyday Experiences* Basingstoke: Palgrave.

Bond, E., & Phippen, A. (2022). *Safeguarding Adults Online: Perspectives on Rights to Participation.* Policy Press.

Bond, E., & Tyrrell, K. (2021). Understanding revenge pornography: A national survey of police officers and staff in England and Wales. *Journal of Interpersonal Violence,* 36(5-6), 2166-2181.

Bronfenbrenner, U. (1979). *The Ecology of Human Development*. Harvard University Press.

Chen (2007). "The politician's fallacy and the politician's apology". https://devblogs.microsoft.com/oldnewthing/20070226-01/?p=27853 [Accessed February 2023]

Citron, D. K., & Franks, M. A. (2014). Criminalizing revenge porn. *Wake Forest L*. Rev., 49, 345.

Cohen, S. (2002). Folk devils and moral panics: The creation of the mods and rockers. Psychology Press.

Cole, T., Policastro, C., Crittenden, C., & McGuffee, K. (2020). Freedom to post or invasion of privacy? Analysis of US revenge porn state statutes. *Victims & Offenders*, 15(4), 483-498.

College of Policing (2015). “Revenge Pornography Briefing Note - May 2015”. http://library.college.police.uk/docs/appref/briefing-note-revenge-pornography-may-2015.pdf [Accessed February 2023]

Crown Prosecution Service (2017). “Revenge Pornography - Guidelines on prosecuting the offence of disclosing private sexual photographs and films.” https://www.cps.gov.uk/legal-guidance/revenge-pornography-guidelines-prosecuting-offence-disclosing-private-sexual

FCC (1996) Telecommunications Act of 1996 available from https://www.fcc.gov/general/telecommunications-act-1996 [Accessed February 2023]

Greenwald, G. (2009). "Drug decriminalization in Portugal: lessons for creating fair and successful drug policies." Cato Institute Whitepaper Series .

Hari, J. (2015) *Chasing the scream: The search for the truth about addiction.* Bloomsbury Publishing.

Livingstone, S., van COUVERING, E., & THUMIM, N. (2006). *Children’s privacy online.* Computers, Phones, and the Internet: Domesticating Information Technology, 2, 128.

Marlatt, G. A. (1996). Harm reduction: Come as you are. *Addictive behaviors*, 21(6), 779-788.

McGlynn, C., Rackley, E., Johnson, K., Henry, N., Flynn, A., Powell, A., ... & Scott, A. (2019). Shattering lives and myths: a report on image-based sexual abuse.

Muffet, A. (2016). “On the Digital Economy Bill”. https://medium.com/@alecmuffett/on-the-digital-economy-bill-1df356862ac2 [Accessed February 2023]

OFCOM (2022). Children’s Media Use and Attitudes. https://www.ofcom.org.uk/__data/assets/pdf_file/0024/234609/childrens-media-use-and-attitudes-report-2022.pdf [Accessed February 2023]

O'Reilly, T. (2009). *What is Web 2.0*. O'Reilly Media, Inc

Pardo, B. (2014). "Cannabis policy reforms in the Americas: a comparative analysis of Colorado, Washington, and Uruguay." International Journal of Drug Policy 25.4 (2014): 727-735.

Phippen, A. (2009). “Sharing Personal Images and Videos Among Young People” Report for South West Grid for Learning available from http://webfronter.com/surreymle/devonesafety/other/Sexting%20report%20-%20andy%20phippen.pdf [Accessed February 2023]

Phippen, A. (2016). “Online Children’s Online Behaviour and Safety - Policy and Rights Challenges”. Palgrave. ISBN: 978-1-137-57094-9

Phippen, A., & Bond, E. (2020). Organisational responses to social media storms: An applied analysis of modern challenges. Springer Nature.

Phippen, A., & Brennan, M. (2020). Sexting and revenge pornography: Legislative and social dimensions of a modern digital phenomenon. Routledge.

Phippen, A., & Street, L. (2022). Online Resilience and Wellbeing in Young People. Springer International Publishing.

Revenge Porn Helpline (2022). Intimate Image Abuse – An Evolving Landscape. https://revengepornhelpline.org.uk/assets/documents/intimate-image-abuse-an-evolving-landscape.pdf?_=1639471939

Ringrose, J.; Harvey, L.; Gill, R. and Livingstone, S. (2013). Teen girls, sexual double standards and 'sexting': Gendered value in digital image exchange. *Feminist theory,* 14(3), 305-323.

Setty, E. (2019). Meanings of Bodily and Sexual Expression in Youth Sexting Culture: Young Women's Negotiation of Gendered Risks and Harms. *Sex Roles* 80, 586–606. https://doi.org/10.1007/s11199-018-0957-x

Setty, E. (2020) *Risk and Harm in Youth Sexting: Young People's Perspectives*. London: Routledge

Trengove, M., Kazim, E., Almeida, D., Hilliard, A., Zannone, S., & Lomas, E. (2022). *A critical review of the Online Safety Bill. Patterns, 100544.*

UK Government (1971). Misuse of Drugs Act 1971. https://www.legislation.gov.uk/ukpga/1971/38/contents [Accessed February 2023]

UK Government (1978). Protection of Children Act 1978. https://www.legislation.gov.uk/ukpga/1978/37 [Accessed February 2023]

UK Government (1992). Sexual Offences Act 1992. https://www.legislation.gov.uk/ukpga/1992/34/section/2 [Accessed February 2023]

UK Government (2015). Section 33, Criminal Justice and Courts Act 2015. https://www.legislation.gov.uk/ukpga/2015/2/section/33/enacted [Accessed February 2023]

UK Government (2017). The Digital Economy Act 2017. https://www.legislation.gov.uk/ukpga/2017/30/contents/enacted [Accessed February 2023]

UK Government (2019). "Online Harms White Paper" available from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf [Accessed February 2023]

UK Government (2021). Section 69, Domestic Abuse Act 2021. https://www.legislation.gov.uk/ukpga/2021/17/section/69/enacted [Accessed February 2023]

UK Government (2022). “Criminal Justice System statistics quarterly: June 2022”. https://www.gov.uk/government/statistics/criminal-justice-system-statistics-quarterly-June-2022

Wood, E., Werb, D., Kazatchkine, M., Kerr, T., Hankins, C., Gorna, R., Nutt, D., Des Jarlais, D., Barré-Sinoussi, F. and Montaner, J. (2010). *Vienna Declaration: a call for evidence-based drug policies*. The Lancet, 376(9738), pp.310-312

Wood, Evan, et al. (2010). "Vienna Declaration: a call for evidence-based drug policies." *The Lancet* 376.9738 (2010): 310-312.

Yar, M., & Drew, J. (2019). Image-Based Abuse, Non-Consensual Pornography, Revenge Porn: A Study of Criminalization and Crime Prevention in Australia and England & Wales. *International Journal of Cyber Criminology*, 13(2).