The UK Government Internet Safety Strategy Time to Listen to the Youth Voice?

Phippen, Andy

Entertainment Law Review
Sweet and Maxwell

The UK Government Internet Safety Strategy – Time to Listen to the Youth Voice?

Andy Phippen and Henry Phippen

The policy space around "online safety" has been active in the last 18 months, with development from manifesto commitment through green paper to proposed white paper. The goal is developing a legislative and regulative programme that will, it is proposed, ensure that UK citizens are "safe" when they go online. With the proposed white paper anticipated in Autumn 2018, it is worthwhile to pause and reflect on the policy direction, drawing from both empirical and personal perspectives on working with children and young people, and what it means to be a young person growing up in this "digital age". By taking these personal perspectives we unpick some of the policy direction and give concrete, practical examples of why we need to address online safety from a more holistic, multi-stakeholder, perspective.

The two authors of this article bring differing, albeit complimentary, perspectives. One is an academic who has spent the last 15 years working with children and young people trying to understand how digital technology affects their lives, as well as working with NGOs, government and education providers to understand how me might be tackle the challenges they face. The other author is a 15-year-old who has grown up in a highly-connected world, and experienced the impact of "online safety policy" from both home and school environments.

The Path to the Internet Safety Strategy

Let us start with a review of recent policy documents that anticipate the white paper. In the 2017 Conservative Party Manifesto[1], there was a commitment to:

"make Britain the safest place in the world to be online"

Within the manifesto the party set out a number of aims to make this possible (without actually exploring what it actually means to be "safe" online), including:

- empowering citizens to "use the Internet without fear of abuse, criminality or exposure to horrific content";
- achieving parity between online and offline behaviour for young people, with specific mention of bullying, engaging in criminal activity or accessing "violent and degrading pornography";
- pursuing technological solutions to these issues on social media sites but also app stores and "content sites";
- making industry accept responsibility to ensure they do not direct users "even unintentionally" to harm or sexual content;
- making industry take responsibility for reporting of upsetting content and take downs;
- making industry provide the tools to tackle extremist content online and facilitate civil society to provide counter narrative and prevent terrorists from communicating online;
- developing new curricula for young people to learn about "the harms of the Internet" and comprehensive relationship and sex education that encompasses online risks such as bullying and grooming.

[1] The Conservative Party 2017. "Conservative Party Election Manifesto 2017". https://www.conservatives.com/manifesto

As we can already see, there seemed to be quite the focus on looking to see what "industry" might do to do implement safety (whatever that might be) online, while ensuring there is no distinction made between online and offline criminal activity. The ideology in the manifesto seems to be that online safety is something that can be controlled through technology, and those who provide the platforms for online communication are responsible to provide this. However, if we take their preferred stance of providing no distinction between online and offline contexts, a slightly facetious offline comparison immediately shows that this is problematic - is a publican responsible to control the discourse that occurs in their establishment, such that they "even unintentionally" are responsible for upset or harm caused there? While the publican might be in a position to intervene in the event of an argument or fight, should they be responsible for pre-emption of the altercation? If this is not a reasonable expectation, why would similar expectation be placed on service providers in the online world?

To make a declaration that the party will make the country "the safest place in the world to be online", without defining what safety actually is, causes some concern – how can we get to a target that we do not understand? A dictionary definition of "Safe", drawing the appropriate designation, is:

free from harm or risk : unhurt. [2]

Was it really the intention of the party to ensure that anyone in the UK who goes online will be *guaranteed* to be free from harm or risk? This seems like an exceptionally ambitious aim, particularly in an environment so volatile and transitory. While "road safety" might be easier to manage in a stable setting (roads, traffic control technology, expectations of base levels of training and education for anyone engaging with this environment), it still does not guarantee safety. It does, at best, mitigate risk whilst having legislation in place to punish those to do not engage with the defined rules or increase those risks through, for example, negligence or danger.

Regardless, following the 2017 general election, the Conservative/Democratic Unionist coalition Government produced an Internet Safety Strategy Green Paper[3] that set out priorities and a call for consultation with stakeholders on the intended policy direction.

The four main priorities established in the paper were:

- *setting out the responsibilities of companies to their users;*
- *encouraging better technological solutions and their widespread use;*
- *supporting children, parents and carers to improve online safety;*
- *directly tackling a range of online harms.*

With three underpinning principles:

- *what is unacceptable offline should be unacceptable online;*
- *all users should be empowered to manage online risks and stay safe;*
- *technology companies have a responsibility to their users.*

So, again, we can see a focus on industry responsibility and technological intervention. The green paper went to great lengths to highlight the technical nature of the online environment and the need

[2] Merriam-Webster 2018. "Safe". https://www.merriam-webster.com/dictionary/safe
[3] UK Government 2017. "Internet Safety Strategy Green Paper".
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/650949/Internet_Safety_Strategy_green_paper.pdf

for industry to "take responsibility" for what goes on across their platforms with the lion's share of the paper focussing on industry as the primary stakeholder for safety.

As a result of the consultation that took place following the release of the green paper, the government's response[4] continued the narrative of technological intervention and responsibilities of industry, while reinforcing this message by stating how "powerless" users feel in addressing the potential harms they face when going online. In total 528 individuals and 62 organisations responded to the consultation and while the Government claimed that the consultation covered a wide range of online safety aspects including:

- *the introduction of a social media code of practice, transparency reporting and a social media levy;*
- *technological solutions to online harms;*
- *developing children's digital literacy;*
- *support for parents and carers;*
- *adults' experience of online abuse;*
- *young people's use of online dating websites/ applications,*

it was claimed that the consultation highlighted three main issues:

1. *Online behaviours too often fail to meet acceptable standards;*
2. *Users can feel powerless to address these issues;*
3. *Technology companies can operate without proper oversight, transparency or accountability, and commercial interests mean that they can fail to act in users' best interests.*

While there is a claim of breadth in the consultation, the aim was to hold industry to account and, it would seem, to gain public support for great regulation of social media and technology providers, as well as more esoteric proposal such as an "Internet levy", which would be paid by social media and technology providers to fund some form of Internet regulation (although the outcome of the consultation was that this particular concept was not well supported). The response also made clear the intentions of the anticipated white paper's legislative instruments:

To cover the full range of online harms, including both harmful and illegal content. Potential areas where the Government will legislate include the social media code of practice, transparency reporting and online advertising.

In addition, it was proposed that new policy areas will emerge, such as

- *age verification to assist companies to enforce terms and conditions;*
- *policies aimed at improving children and young people's mental health, including the impact of screen time;*
- *tackling issues related to live-streaming; and,*
- *further work to define harmful content.*

The concept of how content becomes harmful, while falling outside of the scope of this article, is worthy to pause and reflect upon. While few would argue that content defined by law to be illegal should be censored, there is less clarity of who decides what is harmful. And if there is no transparency on what "harmful content" is, how can we expect legislation to clearly and unambiguously define it?

[4] UK Government 2018. "Government Response to the Internet Safety Strategy Green Paper". https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/708873/Government_Response_to_the_Internet_Safety_Strategy_Green_Paper_-_Final.pdf

Prohibition = Safe?

It is clear, from this policy analysis, that there is a belief that harm occurs *to* individuals online, but there is little comment about the responsibility of the user or that users can be the ones causing the harm. There even appear to be prohibitive solutions being proposed to address the complex issues around children's mental health - we have already seen calls for social media companies to manage children's screen time[5] by the then Secretary of State for Culture Media and Sport, Matt Hancock, even though the "solution" he proposed would be entirely contradictory to the recently implemented GDPR legislation.

Equally, we can see through all of these policy documents that the focus of responsibility lies on the need for technology providers to provide solutions to this harm. Other stakeholders (young people, parents, educators) all "need help" to tackle the causes of these harms, as many feel "powerless". There is a deflection of responsibility that would not be acceptable, for example, in our road safety analogy. Would we ever imagine a parent saying "I've never driven a car before, nor have I taken it upon myself to learn how to do it, but jump in children, we'll see how we get on"?

It is interesting to note that while pornographic content has been a policy obsession of the Government since 2012[6] there is only a single reference to it in the green paper response. With the assent of the Digital Economy Act 2017[7] perhaps the Government now believe with the age verification measures set out in this legislation (that any commercial provider of pornography has to provide age verification) have achieved the utopia of preventing anyone under the age of 18 from accessing pornography?

However, while the legislation has achieved royal assent, and a regulator (the BBFC) has been put in place to monitor the section of the legislation related to pornography, the age verification specifics have not yet been enacted, mainly because there is no agreement of the technical solution. While it was expected that by the time of writing (July 2018) age verification would be in place, it has now been pushed back to the end of the year and there is still no universal technical solution in sight[8]. Moreover, there are serious privacy concerns about the Government handing over responsibility for the technical solution to the pornography industry itself. It is, therefore, somewhat concerning that age verification, an untried solution for UK citizens to verify they are age of majority is being proposed to look at the even more subjective age "limits" on social media sites. If we are struggling to find a way to prove someone is 18, how might we do similar for a 13 year old?

There is equally little reference to peer on peer abuse by young people – whether this be sexting, harassment, coercion or similar. While cyberbullying is tackled to some degree, it is still viewed as something where technology companies should be tackling it, rather than trying to understand the educational and social contexts around abuse among young people. With an appropriate intervention by a social media provider, or a monitoring tool, perhaps we would not need to tackle the more complex side of these behaviours. This has certainly been the perspective of other government ministers, such as Jeremy Hunt and his proposal for mobile providers to scan children's' mobile devices

[5] Phippen, A. 2018. "Legislating Children's Screentime—Surely Not a Solution to Children's Mental Health Challenges?". Entertainment Law Review 2018 (5)
[6] Phippen, A 2016. "Online Safety Policy and Practice 2010-2015". Palgrave.
[7] UK Government 2017. "The Digital Economy Act". http://www.legislation.gov.uk/ukpga/2017/30/contents/enacted/data.htm
[8] Griffin, A. 2018. "Porn Age-Verification Laws Delayed by UK Government Amid Widespread Confusion About How They Will Actually Work. https://www.independent.co.uk/life-style/gadgets-and-tech/news/porn-age-verification-laws-ageid-youporn-pornhub-mindgeek-uk-government-a8251791.html

to “indecent” pictures, discussed in a previous article[9]. Yet, from our work with young people over more than ten years, we know that an issue such as the generation, sending and non-consensual sharing of indecent images of peers is something that they are regularly exposed to, and one that is complex and challenging to address.

Ultimately, the policy perspective is one of prohibition. The view is predominantly “if we can stop this happening, the individual will be safe”. By preventing a situation, by taking down content, by encouraging social media providers to aggressively monitor and censor posts on their sites, do we achieve the goal of a safe online environment? Is the Government confusing “make Britain the safest place in the world to be online” with “make Britain the most prohibitive place in the world to be online”? We see proposals for content control, monitoring, age verification, behavioural management and limitation on screen time all as a result of intervention by the technology provider who is implementing such measures under threat of further legislation if they do not. We are seeing little to propose upskilling the population, addressing the need for effective and broad relationships and sex education in schools, and to make individual responsibility something that a user might be held accountable to in their online behaviours.

We feel we need to take a step back from this ideological obsession with accountability by industry. While we would agree that industry needs to play its part and has to have some level of accountability, we would equally argue that they cannot provide the solutions. All that industry can essentially do is provide users with the tools such as those to report abuse, block abusers and proactively police content that has already been identified as illegal. Unless we are going to expect the need to be “safe” to trump fundamental human rights, anything beyond this is problematic. While some social media providers already define “community standards”, equally they argue that freedom of expression is important, even if some expressions are unpalatable[10]. We cannot expect algorithms to make moral judgements, as algorithms deal with absolutes while morality does not. To expect algorithms to make these judgements reflects a failing in understanding of how the technology works. Let us, for example, reflect on the previously mentioned call for mobile providers to install algorithms on children’s phones to detect self-generated indecent images. Given there is no legal definition for indecency, we have already hit a brick wall algorithmically speaking. Although perhaps we could expect a case based approach to identifying “similar” images, which would unlock a moral tension few private sector organisations would wish to engage – if we are to “train” an algorithm to identify indecent images of children, we would have to show it comparable images. This is clearly not a viable technical solution.

The policy perspective has failed to effectively consider the facet that young people tell us is most important – effective education delivered by knowledgeable and responsive professionals. From our perspective, one of the most disappointing things about this manifesto and subsequent papers has been the lack of focus on education. While both the green paper and response both provided discussion around education there was little commitment to place any developments in curriculum or safeguarding into legislation. There is little to suggest any further support for education, to develop curriculum further and certainly no mention of the need for specialist teachers in this area. And while there was a manifesto commitment to provide comprehensive relationships and sex education this has recently been pushed back to 2020 by the Education Secretary Damien Hinds in a quiet announcement during an Education Select Committee oral evidence session[11].

---

[9] Phippen, A, Brennan, M. and Agate, J. 2017. “Doing More” to End Sexting - Facts, fictions and challenges in the policy debate on young people’s sexting behaviour”. Entertainment Law Review 2017 (2).

[10] Swisher, K. 2018. “Facebook CEO Mark Zuckerberg on Recode Decode“. https://www.recode.net/2018/7/18/17575158/mark-zuckerberg-facebook-interview-full-transcript-kara-swisher

[11] Parliament TV 2018. “Education Committee Wednesday 27 June 2018”. https://www.parliamentlive.tv/Event/Index/58da6df3-da79-4b92-99cb-64a2a96d03de

From a personal perspective as someone who frequently visits schools and talks about online technology and how it affects the lives of the young people I am often met with groans when one mentions “online safety”. While I often discussed this issue with schools, generally staff stress they are “doing their best” but they have little guidance which, coupled with threat from the schools inspectorate to explore how this aspect of education is delivered in the school. This subsequently results in education being generally a mix of resources drawn from NGOs in the area, with perhaps one or two members of staff who have received any training in this area providing extra input.

In considering the gulf between policy position and the realities for a young person growing up in the connect world the government is so keen to make “safe”, there is little better way than presenting the youth voice on this. The following section is provided by a 15 year old male currently working state school education in the South West of England, who has grown up alongside the rapid developments in digital technology. Following this discussion, we will draw together the key issues and how the policy area needs to mature if young people are actually going to benefit from the proposed “solutions”.

A Youth Perspective on the Online Safety Policy Space

Growing up in a world alongside the development of the Internet, it has always felt as though older generations have never really been able to grasp the way in which young people use the Internet for communication, education and recreation, and as a result all online safety education ever presented to me and my peers has felt out of touch and somewhat pointless, simply reiterating the points that we have been told from year 7, with no more depth or new information whatsoever being introduced. Where almost every piece of online safety education has fallen short is in the overly large age range targeted by each resource. The supposedly leading-edge resources offered by organisations such as Childnet and the UK Safer Internet Centre both offer the same resources to everyone between the ages of 11 and 18. This is a massive oversight and leads to anyone above the age of about 13 to find the resources incredibly patronising. This only serves to make young people more likely to ignore the information presented to them, even if some of it may be valuable.

Focusing on the websites of both Childnet and the Safer Internet Centre, I found that while there are a lot of points that are useful and relevant for younger secondary school children (children of between roughly 11 and 13), there is nothing of this sort for anyone older. They seem to forget that a lot of the points they present (people may not be who they say they are, be cautious of how you present your image online) are known by the vast majority of teenagers. Furthermore, some of the actual issues applying to teenagers using the Internet, such as sexting, are avoided and treated with vague language until the resources for these issues are specifically searched for, whereas issues such as these should be promoted by organisations such as these.

The Use of Legislative in Education

One important part of online safety education that was addressed by these organisations, which is usually not taken into account by schools, is that much of the legislation applying to the use of technology was written before the creation of the Internet, and it is not yet adapted to deal with the new issues technology can bring. For example, teenage sexting is technically illegal under the Protection of Children Act 1978, so many adults choose to tell their children if they send explicit images of themselves over the Internet, they could be arrested. However, this law was written before the advent of the Internet or smartphones, and did not take into account the possibility that the image may have actually been taken and distributed by the same person it is of. As a result, with many cases of teenage sexting that have been taken to the police, the incident has been declared as not in the

public interest and no charges have been pressed, unless it is felt that one party involved is potentially vulnerable.

This is a good example of how the law can be flexible and will never really be able to develop at the same rate as technology and the use of technology, so it must be adapted. Instead of telling children that if they are to do something that is technically against the law, they will be arrested and charged for it, both Childnet and the Safer Internet Centre recognise that the law is adaptable and is in fact there to protect children from predators and the police and courts do not want to punish a teenager for sexting, if it is consensual between both parties involved and no children are actually hurt or at risk. This is a step in the right direction in terms of education, but it seems, at least from my own experience, this point is given the least regard by schools making use of the websites and resources provided by these organisations.

Teacher Knowledge and Support

I believe that in some ways this is the fault of the teachers, who receive resources and information that they themselves do not understand, so tend to ignore the more nuanced aspects of digital safety (particularly the relationship between the law and digital safety), as they themselves do not understand it and require further education on the topics prior to them explaining these topics to pupils. This is something that must change. The information provided to older teenagers ought to take more of a descriptive approach, showing what may happen as a result of their actions and taking a more open-ended, discussion-based approach, allowing pupils to share their opinions or experiences.

Part of this issue comes from the way many teachers (specifically members of Senior Leadership) tend to present themselves as disciplinarians, which makes it very difficult for the pupils to feel as though they would care and be there to help if a pupil did something regrettable, such as sharing nude images of themselves, most pupils would avoid going to a teacher for help as they fear it would only cause them to get in trouble. In addition to this, in my experience it is not often I feel a teacher has a good knowledge of the topic themselves, which is another reason the education provided often seems arbitrary and unhelpful. It does seem that the vast majority of the time, the teachers themselves are less confident on the topic than the children they are teaching, which only further makes pupils feel as though they cannot really go to teachers were they to have an issue as a result of their online activity. This can also, in some ways, extend to parents. For example, if a parent was to track and monitor their child and their Internet usage, it would break down the trust between parent and child, leaving the child with no adult to go to should they have done something they were not supposed to. Due to this, while online safety education resources for children are very important, it is possibly more important to offer resources to parents to show them the importance of trust and that, just because these monitoring options are available in our digital world, does not mean they are necessary and they can in fact be detrimental to the relationship between parent and child. As there is a disconnect between what children do online and what adults actually understand, these monitoring options only really serve to create argument, as adults may misinterpret their child's activities based on anecdotes, due to their lack of understanding on the topic, and punish their children for something they have not done, which only further serves to break down trust.

Does Technological Intervention Work?

Another option used to try and keep children safe (or control them, depending on how you look at it) is the use of Internet filtering, which will block certain websites, or categories of websites. Having grown up in a home where no filters were ever used on our Internet, I had no experience with them and no real knowledge of the sites they blocked or how easy it was to get around them. We installed

BT's "strong" filters onto my home network and we attempted to see what we could still find, before attempting to bypass the filters.

While a lot of the categories the filters claimed to exclude were indeed blocked (Pornography, Weapons/Violence, Gambling, etc.), the blocking of drugs-related sites was not exactly effective. With a quick Google search, we were able to access articles on how to produce cocaine and MDMA, without even having to try and bypass the filters; they simply did not block these websites. Following this, our attempts to bypass the filtering system was almost immediately successful. Through any of a number of proxy websites, we were able to bypass the filters and see content that was previously blocked. It was not as though we had to spend time researching how to bypass filters, it was simply common knowledge amongst Henry Phippen's peers that filters can be bypassed via the use of proxies, so within minutes we were able to view all content as though the filters had never been installed in the first place. Amongst those who do have filtered Internet at home, the methods of bypassing filtering systems appear to be common knowledge, with many making use of a VPN or proxy to bypass the filters set by their parents. With this knowledge so widespread, the use of filtering for any child above primary school age is essentially pointless, as if they want to view blocked content, they have the knowledge that enables them to.

It seems as though in a lot of cases, filtering is used by parents as an excuse to avoid talking to their children if they see any harmful content online, ignoring issues thinking that the filters will block any and all harmful content, as though it is the ISP's responsibility to protect the children, which takes away some responsibility from the parent, which is not the best way to treat things. It should not be the responsibility of an Internet service provider to protect people's children. This is an outlook that has been becoming increasingly more prevalent with the advent of the Internet, and simply does not make sense. If a parent was to take their child to a playground, they would not expect it to be the role of the playground owner to protect their children, they would take a more proactive role in caring for their children. This proactivity should apply to the digital world, as well as the physical one, as it is not really the ISP's responsibility. However, some forms of proactivity are not positive at all, such as the ability of parents to track their children's phones. This is possibly the worst thing a parent could do should they want to have a relationship of trust with their child. This sort of monitoring makes children feel as though they can never really enjoy themselves, as they know that their parents are essentially watching them at any time. It does not cause children to be more obedient to their parents either, it only causes them to rebel in more abstract ways. For example, if a parent monitors their child's phone, the child may then use another phone their parents do not know about, so that their parents cannot track them.

Reflections on the Green Paper and Response

A good example of the difference in understanding between the way adults and children view and use the Internet is in the government's Green Paper. One of the points made is that the Internet makes development through a child's teenage years more complex, when this is really not the case. With an almost unlimited wealth of information, as well as the ability to contact their peers at almost any time, the Internet has actually made teenager's development easier, and has allowed them to feel more accepted than previously, as they can find things in common with not only people they know in person, but also people on the Internet. While yes, people may say they are someone different online, most people are who they appear to be online, and this provides a valuable opportunity for young people to join discussions about topics they are passionate about with a vast range of people, with a huge range of opinions. This helps young people to develop more sophisticated opinions on subjects they are passionate about, and helps to shape them into a more unique and understanding person in much less time.

In the paper, the government promote an age-targeted approach. While this is a good idea in principle, it is very easy to get this wrong, resulting in resources and advice that is suitable for the younger end of the age bracket, but feels patronising and is consequently ignore by the older end of the age bracket. A reasonable method of age grouping would be to group based on school Key Stages, therefore grouping Years 7, 8 and 9 whilst having a separate group for Years 10 and 11, as this is much more representative of the development of children, especially compared to the current approach of grouping all secondary school children together that has been adopted by organisations such as Childnet and the Safer Internet Centre. The advice provided on these sites, as mentioned above, is effective for the younger years at secondary school but quickly becomes patronising and ineffective. This is an issue for several comments and resources made by supposed industry experts, all seem rather out of touch, assuming young people are completely unaware and would believe almost anything they see on the Internet, were it not for the resources provided to them. This discrediting of young people's critical thinking and knowledge leads to many finding digital safety education patronising, which consequently encourages them to ignore the information, with young people often finding more use in advice from their peers. This fact is fortunately acknowledged in the paper, as well as the fact that education from authority figures can often be ignored, as they come across as having a poor understanding of what the youth actually use the Internet and technology for. Despite this, throughout the paper's section on young people, there is no input from any young people themselves, which could be considered one of the largest issues with almost all online safety resources and education.

One statistic that I found rather worrying was that were fewer parents worried about their children drinking or smoking (which are actively harmful to their children's health) than there were parents worried that their children would take part in sexting, an activity which, as long as it is between two consenting parties, does not cause any real harm to their children. It is important that not only are children educated on the potential risks of sexting, but also that parents are taught that it is not necessarily a harmful activity for children. While in the majority of circles, teen sexting is viewed as problematic, this is not really the case. If it occurs between two consenting individuals, there is no real issue and no harm is being caused, despite what many parents and media outlets think.

What Do We Mean by "Safety"?

For the majority of young people using the Internet, online safety is not really even the correct term for the education they need. By the time most children leave primary school, they are already aware of the real, physical dangers of the Internet such as the mental health disorders that can be brought about by excessive social media use. However, while most understand this, it is still retaught in a rather heavy-handed way, from my experience implying that social media use is directly linked to depression and body image issues. While this may be true in some cases, the way it is taught to pupils is rather ineffective. Instead secondary school students more so require education that acts performed online can have consequences. This is usually understood by most young people and adults, but the way this is presented to teenagers especially can be very problematic. Many school's attempts to educate their students on the consequences of some online activity amount to little more than fearmongering, exaggerating the severity of many issues and leaving pupils feeling as though if they do something regrettable online, they have ruined their future and have nowhere to go for help, and no ability to resolve their issues. While the online safety resources available online are quite lacking for teenagers, it is much more important that the issue of schools having a poor understanding of the issues around online activity and as a result propagating fear amongst their pupils is addressed beforehand, as this leaves children feeling lost and as though they are beyond help if they make a mistake online.

While the government's paper does take note of mostly the correct topics that children need educating about, it overemphasises the risks of children accessing pornography (something which

many teenagers *choose* to do) and takes an overly vague approach to outlining the changes they will make. For example, the promotion of "appropriate" filtering is mentioned, but it is never said what constitutes appropriate content, and what is appropriate or offensive will always be subjective, so this idea will never really be effective.

However, there are some steps in the right direction, such as the growing acceptance that adults and authority figures will never really have the same grasp of the issues as young people, and the "Digital Leaders" idea is the most promising in the paper, as it will be allowing young people to have their say in the issues regarding digital safety, giving a more effective and accurate range of issues and education than ever before. It would allow young people to have a voice on an issue which primarily affects them, and would help children and particularly adults to achieve a greater understanding of the way young people use the Internet, and what the issues really are.

If the government were to produce a white paper on its Internet Safety Strategy, the most important thing it would need to include, which is currently lacking, is the requirement for open discussion, as well as more education for adults and teachers before they attempt to educate children. Should teachers be more confident and knowledgeable on the topic, their pupils would find the education more enriching, and more detailed, in-depth discussions would be possible. As discussion with young people is essentially required to enable online safety education to move forward, pupils need to be able to feel confident that the teachers engaging in discussion with them are receptive, open-minded and have a solid grasp of the issues. The government would also need to be more specific with the age groupings they advise to avoid content coming across as patronising. In a similar vein, the use of scenarios to educate young people should be reconsidered, and only used in discussion, as there is no one correct way to respond to a scenario, despite what some resources, such as the Safer Internet Centre's Safer Internet Day quiz[12], suggest. It is important the government realises that almost every aspect of digital safety is subjective, and almost everyone will react in their own way, so simply teaching from a list of criteria will always be ineffective; discussion is the way forward.

In Anticipation of the White Paper

Drawing key issues from discussion above, we can see that:

1. A lot of education resources can be considered patronising by older children who feel online safety education is repetitive and lacks nuance
2. Legislation is used to threaten, not help
3. Technological interventions do not work and are easy to bypass
4. Safety is not the correct term – we should focus on critical thinking, resilience and consequences, not being "safe"
5. Education is not one way – a discursive environment is more successful for stakeholders can learn from each other
6. Control is not safety.

Moreover, we need to give young people credit for being self-aware and not passive consumers in the online world. There are unpalatable (for some) issues emerging from this discussion – some teens will seek out pornography, and there is consensual exchange of images among teenagers which they do not view as problematic. While we, as adult stakeholders in this space, might not enjoy reading this, it is a fact. And preventing teenagers from accessing pornography online until the age of 18, even if it were technically possible, will not change this. Similarly, while we might not wish for teenagers to

[12] UK Safer Internet Centre: https://www.saferinternet.org.uk/blog/test-your-online-safety-knowledge-safer-internet-day-quiz.

exchange images with each other, if there is no harm, is this something we should try to prohibit? Would efforts be better invested protecting those who are harmed by the *non-consensual* sharing of images, coerced into generating images or exploited as a result? Or ensuring that relationships and sex education is delivered effectively at earlier ages so young people are aware of the risks associated with being asked to send a nude image, or that such behaviour is not a usual part of the formation of a relationship.

Legislative threats do not work, they have not worked for sexting, as they did not work for drugs consumption or illegal filesharing (which actually reduced greatly once the music industry provided different models for downloading music). However, if we reflect upon the above discussion compared to the manifesto and green paper position we do not just see gaps between what Government believes constitutes "safe" online and what young people understand, we see a gulf in ideology. We should caveat this with a further statement – the view presented above is not unusual in our other work with young people – online safety is not a term young people are comfortable with and feel it is patronising and fails to take into account youth voice.

Young people are not calling for greater responsibility by services providers to proactively monitor their posts and automate take downs should the provider's algorithms deem the post to be offensive. They are not asking for tools to be provided to "protect" them from vast swathes of the online world, with little transparency of the choices made by the tools regarding which sites to block and which to allow. In our experience, young people do have expectations on service providers – they want tools for reporting, that want to see transparency in the outcome of reporting, they want to be able to manage their privacy, and they want to be able to block those they do not wish to communicate with. However, they also have many expectations on the other stakeholders in their safeguarding – for teachers to have effective, age appropriate, resources, for them to be sufficiently trained that they can answer questions young people ask, and for the opportunity in these educational environments to be able to discuss, to be heard and to be responded to. The want teaching staff and other adults in their lives to understand the issues they face on not judge them harshly if, through engaging with risky behaviour, they get into trouble. They want environments where they can disclose fears or harms without concern they will be criminalised as a result.

In anticipation of the White Paper, we do not hold up much hope of a progressive, youth centric approach to the legislative goals that have arguably been drawn out of the consultative process that began with the Conservative Party's 2017 manifesto. While we would hope that we move away from prohibition as the default setting for "safety" we are not enthused by what we have seen to date. Let us hope that in areas such as access to sexual content, there isn't a belief that with our lurching toward ineffective age verification solutions (easily bypassed with proxying which, as we see above, are well known among the teen population) there is no need for any further policy work in this area. While it might be more challenging from a policy perspective to accept this, surely it would be more effective to acknowledge the availability of pornography and provide education that encourages critical thinking and honest conversation, rather than blocking and filtering, which essential just moves the issue into adult social care.

We have a youth voice that is calling for policy that aims not to make children safe but to make them resilient, so they can make judgements on the problems they face, the potential for harm that exists, and the impact the hyper connected, always on, metric driven popularity has on their mental health. We will not resolve these issues by preventing them from accessing certain parts of the Internet, preventing them using certain words, or having social media providers decide they've spent too much time online in a given day. Young people are telling us what they want, why are policy makers not listening?