# Safeguarding Vulnerable Adults Online: Perspectives on rights to participation and protection online.

*Emma Bond and Andy Phippen*

## Chapter 2

## The Context of Online Safeguarding

### Introduction

In this chapter we consider the wider context of online safeguarding. One of the fundamental arguments we put forward in this volume is that a turning point in adult online safeguarding arose with the joint Court of Protection judgements Re A ([2019] EWCOP 2) and Re B ([2019] EWCOP 3), and the subsequent ruling on the appeal against the Re B judgment ([2019] EWCA Civ 913), given that Cobb J spent a lot of time in his judgement considering the nature of online safeguarding and where professionals might go to build a knowledge base around the issues their clients are facing, and the Mental Capacity Act 2005. We explore these judgements below, and subsequently their legacy in more detail in chapter 4, where we also explore the impact of these judgements on the consideration of digital rights afforded to those adults with mental capacity issues.

While the concept of online safeguarding for children and young people is well explored from both research and policy perspectives, and there are many statutory requirements on stakeholders to ensure effective training and education in this area, the same cannot be said for adults with learning difficulties and mental capacity issues, and for those supporting them. Indeed, we find a dearth of academic research, policy direction or practice guidance related to these difficulties and challenges, leaving those with safeguarding responsibilities with vulnerable adults to make poorly informed judgements on their capacity to engage with online services and confusion on how best to support them. Both of the judgements by Cobb J made it clear (and this was most certainly one of the primary motivations for this book) that there

was very little evidence, support or guidance for practitioners working in the adult safeguarding arena that would be effectively applied in these cases. Therefore, Cobb J turned to the more established world of child online safeguarding for guidance and support in making these judgements, something we will explore in more detail later in this chapter.

We feel, however, given that the knowledge base around child online safeguarding so strongly informed the judgements, and they subsequently have informed other judgements, that it is worthwhile to explore the context and history of online child safeguarding, in order to more accurately understand the current landscape. It should be noted that there are many reasons, predominantly political rather than evidence led, that have resulted in the current online safeguarding landscape. Being able to understand those gives us a better understanding of the difficulties in transferring these concepts to the adult context, as well as attempts to steer thinking around adult online safeguarding away from some of the errors made in arriving at current practice in online child safeguarding being predominantly:

- a prohibitive mindset
- based the belief that technology can “solve” the social and emotional issues that arise from online interaction
- privileging the withdrawal of individual’s rights-based issues in order that we might ensure their safety online.

Therefore, in this first chapter proper outlines the trajectory of online safeguarding and the development of the dominance on protecting children and young people in online spaces. It looks at the role of statutory guidance for online safeguarding of children and young people and explores some of the lessons learned in the last decade of academic research, policy directions and it questions how successful we have actually been in practice. We look at perspectives on safeguarding adults and critically consider the rhetoric of multi-agency working to outline the key debates in dominant discourses in online safeguarding in relation to adults and the roles local authorities, health and social-care and law enforcement as well

as non-statutory agencies play in safeguarding practices in the UK. The chapter explores the risks associated with being online, for example, grooming and exploitation (both sexual and financial) as, we know from our research, these are poorly understood. We explore in more detail the concept of *vulnerability* in relation to adults in chapter 7. However, it should be acknowledged throughout this text that vulnerability should be considered a social construction rather than a medical model, and vulnerability will vary depending on disability, capacity and life course.

We examine the current context of the fundamental rights people have to access information, to privacy, to managing aspects of their financial lives and shopping as well as their social lives and relationships online and to the support they need to fulfil these rights whether through official, formal care roles or more informal ones through family and friends. The chapter underpins the development of the following chapters to examine the often-polarised viewpoints of the positive benefits of reducing social isolation, education and learning and access to news and areas of personal interest in contrast to the negative risks from scams, unwanted sexualised and/or violent content and potential harms.

Furthermore, we foreground the text in real life examples of some of the complex dilemmas that professionals, carers and families have faced in confronting online risks such as financial exploitation, emotional distress and illegal content and activity.

## Learning from the Child Online Safeguarding Arena

From our perspective, the Court of Protection decisions in the Re A (Capacity: Social Media and Internet Use: Best Interests) [2019] EWCOP 2 and Re B (Capacity: Social Media: Care and Contact) [2019] EWCOP 3 judgments present some interesting reflections, given our extensive experience (collectively nearly 40 years) in the online safeguarding space, about where the criminal justice system is in relation to protecting those with mental capacity issues and how we might best support them while, at the same time, ensure they are safe from harm.

Furthermore, it is important to remember that we should not assume that vulnerability or specific mental capacity issues mean that an individual will not have capacity to make judgments around *any* area of their life. As the MCA Code of Practice (UK Government 2013b) states:

> A person's capacity must be assessed specifically in terms of their capacity to make a particular decision.

Thus, we cannot assume because an individual does not have capacity in one area of their life, they do not have capacity in others. This is vitally important in considering how decisions are made in relation to online access for people with a learning disability or impaired mental capacity. As we have observed from many years of research and practice around online safeguarding, the problem with the online safety space, as we have already explored elsewhere at great length (Phippen and Bond, 2020; Bond and Phippen, 2019 and Phippen and Bond, 2019a), is in our rush to develop quotable soundbites and simple messaging, we are failing to appreciate the diversity of motivations and behaviours of people, or to treat them as individuals. And the parlance of section 1 of the Mental Capacity Act 2005*i*, where we are assuming a person has capacity unless it has been established that they lack capacity, is very much at odds with this thinking.

However, just as we argue in Chapter 6 that the Online Harms Bill fails to differentiate between the identified *harms*, the Cobb J rulings seem to have established, in both Court of Protection rulings and more widely across social care practice, that the *internet and social media*, is a single act, rather than the underpinning technologies for a wide range of services, behaviours and actions. One does not *do* social media, one uses social media to interact with friends and family, to follow interests, to keep track of current affairs, etc. The internet is even more broad, providing the connecting technology for social media platforms, but also communication, gaming, accessing information, watching TV and movies, shopping, social connectivity for

family, friends and strangers, dating and so on. While the MCA might drive thinking toward consideration for the individual, rather than blanket judgements, defining *internet and social media* as a single, broad concept is a step backwards which masks both the reality and the diversity of online provision and usage. We should, instead, be considering whether an individual has, for example, capacity to use digital technology specifically for making new friends or dating, for example, or for making financial transactions or accessing information or entertainment.

While we admire Cobb J, and others involved in these rulings, wishing to base their decisions upon an evidence base, as opposed to (the frequently adopted but little recognised practice of) bringing their own opinions, value biases and media shaped thinking, we do have concerns that basing adult online safeguarding upon the more established field (both academically and legal) of child online safeguarding, risks repeating the mistakes of the past.

Given the many years of research, policy decision and stakeholder practice in online safety, our own experiences show little deviation in findings from discussions with children and young people in 2005-09 (Phippen, 2009 and Bond, 2010; 2013; 2014) to the present day (UK Safer Internet Center (2017). Given that youth discourse has not developed or matured in well over ten years, we would, quite rightly, question whether the thinking and discourse within online child safeguarding in this time has been effective. Surely, if things had progressed, young people would have a different perspective now?

Within the child safeguarding arena, for example, those who wish to protect remain, firmly rooted their narrow viewpoints rather than to listen and educate, and policy perspectives move little beyond victim blaming, apathy and engagement with risk discoursers even though prohibitive messages have been delivered to young people for over 15 years with little meaningful impact. If we are to consider a well-researched, and debated, aspect of online child safety – teen sexting (the exchange of intimate images by teenagers) – we know from

our empirical work that the key educational message was, '*don't do this, it's illegal!'.* Clearly, this has certainly not been effective (Phippen and Bond, 2019b)! At the time, young people were calling for education and routes for disclosure that would not risk them being criminalised. Despite online technology having a taken for granted, ubiquitous role in everyday relationships (Ling, 2012) including intimate relationships (Bond, 2011; 2014), in the UK Government's 2019 curriculum definition for Relationships and Sex Education (DoE, 2019: 30), which finally became statutory, the only mention of teen sexting in the whole document lies in the section on *The Law,* accompanied by the rather chilling statement:

> There are also many different legal provisions whose purpose is to protect young people and which ensure young people take responsibility for their actions.

Rather than continue to repeat and reinforce victim blaming rhetoric, we see, and we indeed hope, that with the Cobb J judgments and the wider debate that has emerged, an opportunity to not make the same mistakes of child online safeguarding and over-protectionist approaches, but to take a victim centric approach that does more than provide victims with finger wagging and shrugs. This book, therefore, aims to encourage an approach that leaves what we might refer to as *digital unconscious bias*, out of professional judgements and instead introduce a perspective that considers the rights of the individual – their rights to participation, and to privacy, not just to protection - critical thinking, and a cognisance of their best interests.

## Re A and Re B

The 2019 Court of Protection judgments on Re A (EWCOP 2, 2019) and Re B (EWCOP 2, 2019), and the subsequent ruling on the appeal against the Re B judgment (EWCA, 2019), have provided much food for thought around the online safeguarding of adults with mental capacity issues. They, once again, raise questions on the efficacy of legislation in general for protecting victims and the public at large, and from a more academic perspective, raise questions around why the law struggles so fundamentally to effectively tackle online harms.

Furthermore, it allows us to reflect on the challenges of policing online behaviour, particularly those who are vulnerable (whether they be children and young people or adults) without detrimentally and disproportionately affecting their fundamental human rights.

While there are some aspects of the judgments that fall outside of the scope of our focus here to see the direction of travel for online adult safeguarding where the individual has mental capacity issues, there are overlaps (such as sexual consent and accommodation provision) that are meaningful to explore. However, the intention of this analysis is not to conduct a detailed exploration of the judgments, but rather to explore them in the context of the foundations upon which they were built – child online safeguarding – and to review how these rulings and the subsequent "test" of crucial values might better progress adult online safeguarding and avoid some of the well-established but often conveniently overlooked pitfalls of the child online safeguarding space.

There is much to admire in the judgements. We can see from Cobb J's judgments that these landmark rulings acknowledge the struggle with the balance in acknowledging the individuality of each case when set against "rules" that might be applied in subsequent cases and how *Best Interest* (as also set out in section 1 of the MCA 2005) might effectively be applied in future cases that might draw upon these judgments. The Re A and Re B judgments have, in their considered discussion and measured thinking, demonstrated that adult online safeguarding presents many challenges that are not faced in the child online safety world, particularly around the responsibilities of stakeholders or clear legislation given the lack of statutory safeguarding requirements. Or, to put it another way, without the statutory framework that exists around child online safeguarding, there is opportunity to bring critical thinking to judgements and focus more effectively on individual need, interests and wellbeing.

Within the child online safeguarding arena stakeholders are bound by statutory instruments such as the Keeping Children Safe in Education (UK Government, 2018) guidance and

legislation clearly setting out protection of children (for example the Protect of Children Act 1978 (UK Government, 1978) ,Sexual Offences Act 2003 (UK Government, 2003) and Serious Crime Act 2015 (UK Government 2015a), however, within the adult safeguarding arena the legislation around stakeholder responsibility is less clear. The Care Act 2014 (UK Government, 2014) makes no mention of online safeguarding provision and the Mental Capacity Act 2005, while empowering to those with mental capacities issues, does not attempt to define how online safeguarding might manifest (which is beyond the scope of the legislation).

## Applying the *3Cs*

Cobb J develops this thinking by detailing a test that could be used in future cases to consider whether an individual has capacity to make decisions on online risk and, again, this is, in many ways, to be applauded. However, in developing a test that might be applied to future cases, we note that Cobb J refers to the UK Council for Internet Safety's *Child Safety Online: A Practical Guide for Providers of Social Media and Interactive Services* (DCMS, 2016) as a foundation for the test's development. The basis of this argument falls on the concept of the *3Cs,* a long-applied tool in the child online safety space (Livingstone and Haddon, 2009):

> **Content Risk**: children receiving mass- distributed content. This may expose them to age-inappropriate material such as pornography, extreme violence, or content involving hate speech and radicalisation;
>
> **Conduct risk:** children participating in an interactive situation. This includes bullying, sexting, harassing. Being aggressive or stalking; or promoting harmful behaviour such as self- harm, suicide, pro-anorexia, bulimia, illegal drug use or imitating dangerous behaviour. A child's own conduct online can also make them vulnerable- for example, by over- sharing their personal information or by harassing or bullying themselves.

> **Contact risk**: children being victims of interactive situations. This includes being bullied, harassed or stalked; meeting strangers; threats to privacy, identity and reputation (for example through embarrassing photos shared without permission, a house location being identified, someone impersonating a user, users sharing information with strangers); and violence, threats and abuse directly aimed at individual users and/or groups of users.

These definitions have long been adopted (and indeed further updated) in the online child safeguarding world. They are, on occasion, a useful tool to begin a discussion around online risk for young people. Indeed, they broadly categorise the nature of online risks, to a certain degree. However, as we have already stated, building the foundations for vulnerable adult online safeguarding on child-centric approaches is not without its problems or its tensions. We argue that the 3Cs is a simplistic model that assumes a passivity of child and the victim-centricity of approach. Dominance discourses in the social construction of childhood depicting the child as innocent and in need of protecting (Jenks, 2005), it assumes that the actor of these behaviours, whether content, conduct or contact, will be a victim of abuse or harm, rather than a perpetrator. While the Conduct aspect of the rules implies a more active role by the child in an online scenario, it still views this from a position of placing oneself in a position of vulnerability as a result, not that they might be the instigator of abuse, and the actor causing the harm. However, there is a considerable body of research which evidences that *the child* is both victim and threat (Gittens, 1998 and James, Jenks and Prout, 2010) literally and metaphorically. As we have already suggested, the legislative framework for adult safeguarding is far less well defined and, in the event of the subject of care being found to be offending, the legislation is less likely to protect them from prosecution. While there are exceptions to this, such as the exchange of intimate images, where the law for adults protects victims of non-consensual sharing, whereas there is a risk for minors that, because the law that “protects” them – the Protection of Children Act 1978 (UK Government, 1978) - makes no

provision for the subject of an image to also be the sender of an image and the distributor of an image (Phippen and Brennan 2020). However, in general, it is more likely that a vulnerable adult will be pursued for arrest or charge in the event of an online harm than a child.

Interestingly, Cobb J raised the complexity and uncertainty of online law in his judgment Re A:

> 7. There is acknowledged public uncertainty of the law surrounding online abuse; although criminal offences do cover illegal online activity, it is acknowledged that the legislation as a whole requires clarifying, consolidating and/or rationalising in order to be more effective. It is notable in this regard that while it is a crime to incite hatred because of religion or race, it is not presently a crime to incite hatred because of disability. Those who press for a change in the legislation in this regard have a compelling case.

Therefore, while we might view the 3Cs as a useful starting point to develop understanding around what online risk might be, it fails to acknowledge the nuance and individuality of any given "online risk" scenario and, arguably, results in attempts to disregard such complexity in our efforts to fit a risk into its appropriate "C". It reflects a wider wish, explored below, in the online harms policy area, for easy answers to complex situations. A young person taking an intimate image of themselves, sharing it with a consenting partner, who then shares it, non-consensually, to peers, is complex. The dominant westernised view of childhood as non-sexual (James, Jenks and Prout, 2010) and the consistent policy position of '*don't do it, its illegal'* has clearly failed a whole generation of young people, because it blindly follows a piece of legislation that is no longer fit for purpose and a prohibitive mindset that hopes its unquestioning adherence to this law will stop young people doing something that as a society we'd rather they did not. Rather than accepting that this is something young people do as part of their everyday intimate relationships, as victims of non-consensual sharing who deserve as much protection as adults do in a similar situation.

We can see this mindset tending toward prohibitive approaches applied to other issues of complexity, where the morality of the prohibition is easier to justify in a child safeguarding environment than an adult one. For example, let us take a perennial moral quandry – online pornography. If we take this from a child centric safeguarding perspective, we have a simple message – "this child is accessing pornography, therefore let's filter their internet access to prevent this". While this is the subject of much debate, especially around the fluctuating Age Verification legislation (UK Government, 2017) as a *solution* to this social ill, it is difficult to argue that a child *should* have access to pornography. Yet is well established that children access sexual content for information, sexual gratification and acceptance in social groups (Bond, 2014 and Setty, 2020). And, as will be discussed below, there are complexities in the prohibitive approaches with child access to pornography (in that they, in general, do not work!), it becomes a far more complex rights-based issue if we consider this for an adult wishing to access pornography, which is their right as long as the content they are accessing is not extreme pornography or child abuse material. While we might take a perspective that we would rather an adult with learning difficulties does not access pornography, if we take a subjective view based upon our own value biases, it is a far more difficult think to rationalise as "we'd rather they didn't" and it certainly would be difficult to demonstrate that this is in the best interests of the individual. This is acknowledged by Cobb J in his judgments.

## Digital Unconscious Bias

As we have stated already, we draw extensively upon our own empirical work in this area. We do, as a result of our work, spend a great deal of time working with both those for whom the need to safeguard has been identified, and also with many stakeholders in that safeguarding arena. As such we are often placed in situations of debate around balancing the wish to keep an individual safe from the risk of harm with their rights to experience life to the fullest and, as such, should be allowed to engage with the risks in order to also recognise, understand and learn to manage risk. We present below three scenarios that have arisen within our work. The

first was a conversation with a social care team who had responsibility for the care of a young adult male with mental capacity issues related to Autistic Spectrum Disorder. This conversation went some way to highlight the lack of knowledge of online safeguarding, or clear guidance to, those stakeholders with safeguarding responsibility, result into some truly concerning responses that fit squarely into what we have referred to elsewhere as the *Safeguarding Dystopia* (Phippen, 2016).

In this case the social care team was recounting the challenges of caring for this young man, who was living independently but the team had concerns regarding both his use of online technologies and also the risk from harm arising from independent living. Their *solution* (for it is a solution only in the broadest definition of the term) was to place a series of online cameras around the young man's home so they could monitor him remotely while, they perceived, "allowing" him his independence.

> *'The trouble is,' we were told by one of the team, 'we keep on seeing him masturbate'.*

Not only is this illustrative of Rogers' (2016), observation that sexual pleasure for intellectually disabled people is often mediated through surveillance and governance and societal attitudes to disability and sexuality more generally, but also a very clear, uncomfortable, demonstration of how, in the emergent age of casual surveillance of society (see, Lyon 2001), technical solutions with little care for an individual's privacy can also be applied to vulnerable adults. In order to ensure this young man was "safe" those stakeholders with safeguarding responsibilities decided the only solution was to strip him of any right to privacy and provide an approach that was clearly not in the best interests of their client. However, they did perceive that the erosion of the young man's rights was justifiable to make sure he was not at risk. A phrase we often hear is "safeguarding is more important than privacy". The perspective seems to be that as long as the erosion of rights comes from a good place, it cannot be a negative

thing. Moreover, it was only because of their own discomfort in watching their client masturbate that they wished for guidance on how they might tackle this situation. Suffice to say we suggested that the surveillance was excessive, failed to address the client's best interests and should be removed. We suggested instead that regular conversations with the young man about his online activities, alongside an education programme and routes for reporting, might be a more appropriate approach.

In a different case we were asked to advise on a safeguarding concern for a vulnerable adult male who had a care team around him, who were concerned he was visiting the local library to access (legal) pornography. His condition meant he had trouble understanding that the public viewing of pornography was unacceptable or might make others feel uncomfortable. The care team's view was that this was (unsurprisingly) unacceptable and he was upsetting other library users and they wanted to know how they might stop prevent their client accessing pornography. The library, unsurprisingly, was proposing banning him from the setting unless he stopped accessing pornography there.

We did query why he had to go online to access information and content at the library, and whether this was the only means for him to go online. We were told he did have a laptop but it was '*full of viruses'* and was not workable. When asked why they had not had the laptop fixed, it was the view of the care team that if they did that, he would be able to access pornography on it. At no point did the care team provide a rationale as to why this adult male might have a condition that meant accessing pornography would be harmful to him, they just wanted to stop him doing it. The main concern of the care team was that the gentleman should be prevented from accessing pornography, even though there was nothing to suggest that what he was looking at was illegal or there was any professional view that viewing legal pornography would have a negative impact upon his wellbeing. The view was expressed that perhaps preventing the gentleman from accessing pornography was, of itself, a contravention of his human rights, and the focus of concern should lie with rectifying the issues with his

laptop and install anti-virus software so he was not compelled to try to access pornography when he visited the library. We also observed that the library was within its rights to prevent access to certain types of content on their public network, but the gentleman himself should not be prevented from *any* access to legal content just because the care team found it unpalatable. Furthermore, banning him form the library also meant preventing him from reading the comic books and magazines he enjoyed reading and could not afford to buy and to talking to some of the regular library staff and others with whom he like to chat to.

Our final example case is drawn from one we encountered, when delivering training to early career social care professionals, namely a concerned individual who was uncomfortable with what he saw during his first work placement. He told us that he worked in a residential setting for adults with learning difficulties. The senior managers in the setting were concerned about the potential harm that could arise from residents using digital technology, and one had been the subject to financial extortion as a result of an online scam. The management solution was, therefore, to instigate a "spot checking" regime within the setting, so staff would conduct checks on the devices of residents, supposedly whenever they wished to but in reality, it was more likely to take place at scheduled times of day, to ensure they were engaging with online services free of harm and risk.

We should stress that all of the residents of the setting were adults, and none were subject to any Court of Protection rulings that had indicated that they did not have capacity to engage with online content and services. When the professional we were discussing this case with raised concerns about the potential breaches of privacy (and potential data protection risks) associated with this practice, they were told that it was acceptable because all residents had *consented* to these checks and, besides, '*safeguarding trumps privacy rights'*. Perhaps the most uncomfortable thing about this practice was the belief that consent had been received, given some of the learning difficulties experienced by some residents, and the fact they,

essentially, had little choice – what would have happened if one of the residents had not consented? Or perhaps the organisation is confusing consent with assent?

In each of these cases we see a clear demonstration of:

1. A failure to appreciate the rights of the vulnerable adult
2. A view that technology can solve any safeguarding concerns
3. Taking an approach where perceived solutions are in the best interest of the care team, rather than the vulnerable individual

Clearly these brief case examples demonstrate the need for guidance for organisations and for those working with adults with mental capacity issues about how they best support clients while ensuring their rights are protected and the care provided in their best interests. We discuss how to best support clients while protecting their rights in more detail in chapter 7, but note here that these examples are why Cobb J's joint ruling on Re A and Re B is welcome. What is also clear from our analysis of the judgment(s) is that if we are to consider the issues for a single individual in detail, it can be extremely complex and require a careful balance between the rights of the individual, care toward that person, the need to safeguard both them and potentially others, as well as any legislative position. Therefore, this is not something that can be applied to the population as a whole with an algorithm or a universal prohibitive approach. However, this sometimes flies in the face of those working in a safeguarding capacity who are looking for clear and easily applied rules in all contexts.

We also acknowledge and draw attention to the fact that the concept of safety in the online safeguarding world is a strange one, and while we will undoubtedly refer to "online safety" through this text when discussing practice and policy, it is not a term with which we are comfortable. This is because while other safety paradigms are well established, and we can see how the language of safety has transferred too readily to the online world it is in reality somewhat problematic. If we take, for example, road safety, we can see clear operational

solutions to these issues – impose laws of road users, coupled with significant sanctions should they wish to flout them, have an established environment (for example using standard road markings and signage) that is consistent across the legal jurisdiction, and simple education and training programmes to help those who might be considered vulnerable (for example, children and young people) to navigate this environment effectively. We can draw from the seminal work of technology lawyer and academic Lawrence Lessig, in understanding why these approaches work effective in the physical space but are less effective in the digital environment. Lessig (2006: 5) laid out a very clear, albeit challenging, argument around efforts to regulate the online world, arguing that controlling behaviour online is not possible, due to the nature of the environment in which the behaviour took place:

> The claim for cyberspace was not just that government would not regulate cyberspace—it was that government could not regulate cyberspace. Cyberspace was, by nature, unavoidably free. Governments could threaten, but behavior could not be controlled; laws could be passed, but they would have no real effect.

Lessig (2006) argues that in order for a regulatory environment to be a success, there were four key *modalities*:

| | |
|---|---|
| 1. Laws | 2. Social norms |
| 3. Market | 4. Architecture |

We lightly draw on Actor Network Theory (ANT) here (see Latour, 1994) to describe how all of these modalities have a significant role to play in managing and regulating a particular aspect of society, for the benefit of all. The applicability of ANT models to the practical understanding of what otherwise would seem a heterogenous collection of materials (see Strathern, 1999) is pertinent here as within the physical world, these modalities work, because they are clear and adhere to natural law (physics, biology, acceptable moralities), and legislation works, because it can be applied to a physical space (i.e. a country, a community, a road network) without ambiguity. We have already described road safety using these modalities yet if we try to do the same for an online environment, we are faced with significant challenges. Within the online world, the *architecture* that exists is *code*, the raw material of digital technology (while we acknowledge that digital technology also relies on hardware – communication networks and physical devices – they are essentially non-functioning collections of wires and rare earth metals without the code to make anything happen) and the hardware upon which the code communicates. Code designed, written, and shaped by those with the skills, knowledge and talent to be able to turn the requirements of users into functional algorithms and assemble them into software platforms. These software platforms form environments for people to interact in various forms, whether they be social or business, and as a result of these interactions, risks arise (for example, when one member of an online social community becomes abusive to another). Thus, through an ANT lens, the network is heterogenous *actants* – human, social and technical (Latour, 1999) as such the platforms, and code, can put countermeasures in place to mitigate the risk of the abuse taking place, such as providing the potential victim with tools to be able to block and report the abuser, the code cannot, of itself, prevent the actual behaviour of the individual (human).

Lessig's primary idea is that code becomes, in essence, the law of the online world, because it is the only way *rules* can be implemented. Hutchby's (2001a) concept of *affordances* is also helpful here in that there are boundaries to what code can achieve, constrained by logic and the implementation of biases of those who implement it. Code cannot implement ambiguity,

imprecision or morality. It cannot only make a judgement on the behaviour of an individual based upon the data it has been presented with, and that judgement cannot be subjective. Regardless of the current excitement around the potential of artificial intelligence (something we will explore in more detail in chapter 5), there is nothing intelligent about what these algorithms do, they simply follow rules and data, and imply intelligent decision as a result. It, or more accurately, coders, can only implement things that can be defined in a logical manner, and this presents significant challenges when tackling social issues, where system boundaries can be infinity and behaviour is unpredictable.

Returning to online safety, we can argue strongly that we cannot hope to keep people safe online in the same way we try to in a road safety context. If we start from a position of guaranteeing safety online, we are doomed to fail. We can, however, help those who engage with online platforms understand the risks associated with this engagement, and provide them with the information, knowledge and tools to mitigate those risks. The tools might be part of the architecture – the aforementioned reporting and blocking tools, or they might form some kind of education initiatives. However, we would also argue, and will present an analysis of this in this chapter, that the policy position around child online safeguarding has been one of *ensuring* safety for the last ten years, and that has brought us to a position where there is a belief that risk should not be mitigated, but eliminated. This, in turn, results in use ending up with strange and unusual safeguarding judgements and a goal that can never be achieved.

## How Did We Get Here?

> 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 above quotation is taken from John Perry Barlow's (1996) *Declaration of Independence for Cyberspace*, a much-cited *manifesto* that claimed Governments would always fail to control the online world. 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 true). *Internet Libertarians*, who wished for a free and neutral digital world, felt these early attempts to control online communications and place it in a competitive space, were doomed to fail. The declaration continues:

> 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.

Yet, over 20 years after this declaration, we see increasing attempts to *regulate* the online world – applying geographically distinct legislation to a global phenomenon that evolved and emerged through convergence and mutual interest, rather than commercial interests and market forces. Commerce and governments only discovered the internet once it was established, and therefore had little chance to exploit it or regulate it as it grew. This declaration does bring attention to an interesting tension between online technology and the need for governments to govern, and pass legislation that protects citizens from potential harms and regulates their antisocial behaviour. We would not take exception to this. The Declaration of Independence for Cyberspace is not so much a claim that *anything* that happens online cannot be regulated, more that trying to legislate to change the infrastructure and technology of the online environment will neither achieve its aims or be effective legislature. We have already discussed above how Lessig's perspectives on technology regulation support this position – if one cannot control the modalities of regulation, or if some of those modalities do not even exist, regulation is doomed to fail.

Understandably, governments wish to mitigate risk and reduce harm for those going online, and to ensure they are *safe* and this desire ameliorate risk and harm impacts on organisations providing care, services and support to vulnerable individuals. We are supportive of this position. We are not proposing a position where anyone should be allowed to do anything online without risk of punishment. There are, in the more unpleasant areas of social media, many people who believe freedom of speech means they should be able to say anything they wish (Howard 2019). However, they fail to grasp that freedom of speech does not mean freedom from consequences. If, as a result of their wish to express themselves freely, they end up projecting hateful communication, it is right that should be punished for this. However, we are also sufficiently experienced and knowledgeable in the online safeguarding area to know that regulation that fails to understand the underpinning technologies, or believe that these same technologies can tackle what are, in essence, social problems, they are doomed to fail.

There is a famous cybersecurity practitioner, Marcus Ranum (Cheswick, Bellovin and Rubin, 2003), who is much quoted as saying '*You can't solve social problems with software'*. Sometimes referred to as Ranum's Law, this is something with which we would wholeheartedly agree, and something we will explore below and in more detail in chapter 5.

Arguably, the drive to keep citizens "safe" online, particularly from a policy/legal perspective, has, at its core, arisen from a wish to prevent children from accessing pornography. All that has followed in the policy area began with discussions that formed in the UK with an All-Party Inquiry into Child Online Safety in 2012 (Independent Parliamentary Inquiry into child Protection, 2012) which was the catalyst for a speech made in 2013, by the then British Prime Minister David Cameron (UK Government 2013a). In this speech Mr Cameron stated:

> I want to talk about the internet, the impact it's having on the innocence of our children, how online pornography is corroding childhood and how, in the darkest corners of the internet, there are things going on that are a direct danger to our children and that must be stamped out. …

Mr Cameron continued with proposals how to tackle each problem – two issues we would argue are very different, regardless of the proposals that seemed to suggest a similar approach to both. Firstly, tackling child abuse images online:

> You're the people who have worked out how to map almost every inch of the earth from space who have developed algorithms that make sense of vast quantities of information. You're the people who take pride in doing what they say can't be done. You hold hackathons for people to solve impossible internet conundrums. Well – hold a hackathon for child safety. Set your greatest brains to work on this. You are not separate from our society, you are part of our society, and you must play a responsible role in it.

Clearly, access to child abuse imagery is a challenge online and one where there are very clear legal definitions. This is illegal content, unquestionably. However, Mr Cameron also refers to tackling youth access to online pornography:

> By the end of this year, when someone sets up a new broadband account the settings to install family friendly filters will be automatically selected. If you just click "next" or "enter", then the filters are automatically on. And, in a really big step forward, all the ISPs have rewired their technology so that once your filters are installed, they will cover any device connected to your home internet account. No more hassle of downloading filters for every device, just one click protection. One click to protect your whole home and keep your children safe.

A far less clear scenario legally speaking. There is nothing illegal in a child accessing pornography, but it is a behaviour where there is a view (and one we would not disagree with) that children access pornography can be harmful. However, Mr Cameron, by combining the two very difficult types of content access in the same speech, seems to propose they are similar in terms of approach to prevent access.

This direction focused upon the use of technology to solve issues related to online child protection and safeguarding. The view being that given the online environment presents *risks* or *harms* (for example, access to inappropriate content such as pornography, access to harmful content that might relate to images of self-harm and suicide, abuse via messaging and chat platforms or the sharing of a self-generated indecent image on a minor) that might ultimately harm the child in some manner, the technology must also be able to provide the solution to prevent these things from happening (a point we explore further in chapter 6, *Pro-Harm Content Online*). The focus in the early foundations of this policy direction was the prevention of access to pornographic content by children and young people. The solution was seen to be filtering technologies, which would identify pornographic materials and prevent access.

Digital technology is certainly very good at clearly defined, rule based, functionality in easily contained system boundaries. Or, to put it another way, data processing, analysis, and pattern matching of data – looking for things they know about and finding them in big unwieldy systems. Computers are very good at taking data and analysing it based upon rules defined within the system (for example, identify words that *might* relate to sexual content). However, they are far less good at is interpretation, *intelligence*, and inference. What computers cannot do is something they have not be instructed to do. Everything they do has to be defined in code, which requires it to be defined in a manner that cannot be subject to interpretation.

By way of an illustrative, albeit mischievous but useful, example, let us consider the word '*cock*'. This is a term that *might* related to a sexual context – it could refer to male genitalia. Equally, it might refer to a male bird. If we consider this from the perspective of a filtering system, that might be tasked with ensuring an end user cannot access websites of a sexual nature, we might provide that system with a list of keywords that could indicate sexual content. "Cock" may be one of these terms. The filtering system will be very good at pattern matching this string of characters to any mentioned within any given website and will successfully *block* access to this content. However, it will be far less good at determining the actual context of the website – it *might* be about sexual activity; however, it might also be about poultry or livestock.

Even with this simple example, we can see how it might struggle to prevent access to all sexual content or, equally, result in *false positives* – blocking innocuous (we use the term *innocuous* sites to describe those who have been incorrectly blocked based upon the requirements of the filter (for example, pornography, gambling, drugs and alcohol) and not *legal*, because access to pornography is legal in the UK sites that are not 'inappropriate' for children to see (also referred to as overblocking). Given the policy direction, and the pressure exacted upon service providers as a result, it is likely that algorithms will be implemented to be conservative in their filtering – worrying less about overblocking and more at ensuring as much sexual content as possible is captured. A simple and popular example of this comes from the overblocking of the Northern English town of Scunthorpe (Wikipedia, online), given that a substring of its composition is a vulgar word for female genitalia.

From a human rights perspective, these pro-active filtering approaches have already attracted the concern of the United Nations, with the *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* ( UNHRC, 2018) stating that:

> States and intergovernmental organizations should refrain from establishing laws or arrangements that would require the “proactive” monitoring or filtering of content, which is both inconsistent with the right to privacy and likely to amount to pre-publication censorship.

Nevertheless, there seems to be an increased focus on interceptional content moderation from platform providers, and an expectation to monitor behaviour on these platforms in a more pro-active manner (with automated intervention), with the threat of legislation should these calls not be heeded. This is a policy focus that began with young people’s access to pornography, and the unacceptability of this but the policy legacy has continued to demand the technical solution to tackle any form of online safeguarding.

This can be clearly seen in the fluctuating age verification debate in the UK (at the time of writing, it seems the UK government, and some European governments, have decided that this is a good way to prevent access to pornography again (Politico 2021). Legislation was established in the UK in *The Digital Economy Act 2017 Part 3* (UK Government, 2017) that mandated providers whose services provide commercial access to pornography must implement age verification technology such as to ensure no UK citizen under the age of 18 could access their content. To take this seemingly simple example, let us consider how we might prevent children from accessing pornography. From a logical perspective, there are two main requirements in order to achieve this:

- We know the age of the end user
- We know that a piece of content is pornographic

If we can achieve this, we can prevent children from accessing such content. However, if we take each point in turn:

- Unless we have some means for all citizens to be able to demonstrate their age in a digital form how do we know their age? There is not a universal, statutory, identity token that exists in the UK that everyone can use to demonstrate their age.

- Can we define, in logic, what makes a piece of content pornographic, if we cannot even define it in law? While attempts to define in law do exist these are of themselves ambiguous, and the subject of much case law. Case law exists because the law is complex and requires debate and discussion by intelligent people to interpret the legislation and build, on a case-by-case basis, knowledge around the legislation's application to a society. However, in this case, there is an expectation that an algorithm can determine whether one of a potentially massive volume of online content contains pornographic material?

Reidenberg's (1997) work on the *Lex Informatica* very clearly pointed out the need for this understanding. He argued that digital technology imposes its own rules on how data is communicated, and what is possible in this management:

> The pursuit of technological rules that embody flexibility for information flows maximizes public policy options; at the same time, the ability to embed an immutable rule in system architecture allows for the preservation of public-order values. These tools can lessen a number of problems that traditional legal solutions face in regulating the Information Society. Yet a shift in public policy planning must occur in order for Lex Informatica to develop as an effective source of information policy rules. The new institutions and mechanisms will not be those of traditional government regulation. Policymakers must begin to look to Lex Informatica to effectively formulate information policy rules.

Put simply, as we outline above code is good at some things, and poor at others, and the public policy space needs to understand where these strengths and weaknesses lie in order

to make effective legislation to tackle social issues. Most importantly, they need to understand that code cannot solve *everything*. By the end of 2013, the UK Government had forged an agreement with the largest four ISPs in the UK, under which the ISPs committed to offering all new customers a network level filtering service, in the face of a threat to ISPs that if they didn't do something voluntarily, the Government would legislate.

The focus of responsibly lay with industry, and the threat of legislation loomed if they were not to do what they were asked. Therefore, by 2013 all major Internet Service Providers provided a suite of filtering solutions to households to ensure that children could not access pornography on home devices. After considerable government pressure, new subscribers had a default "opt in" to these services – when they establish a new connection the filters are switched on, and the subscriber has to make an active choice to switch them off. Existing subscribers were given the choice to install filters. This voluntary response to policy pressure was put in place in 2013, so has now be available to subscribers for over 5 years. OFCOM's Media Literacy report of 2018 (OFCOM, 2018) reported a figure of 34% of parents of 5-15 year olds installing filters. After 5 years of media reporting, service provider and government nudge and policy drive, filters were still not used being used in the majority of the homes in the UK. The same report stated that over blocking was rarely a reason for parents not to install filters (the most popular reason being they preferred to establish their own *rules* in the home for addressing internet access). Which does raise the question – if these technologies are effective, why wouldn't parents install them in the home?

Within this first wave of pornography prevention *solutions* we also saw the introduction of Family Friendly WiFi (Friendly Wifi, online) – in order that public WiFi access in the UK was filtered to prevent access to Child Sexual Exploitation and Abuse Material (CSAM/CSEM) and pornography (and other "inappropriate" content):

> Simply tell us what type of websites you want to block - Adult Content, Illegal Content, Streaming Media, Chat & Instant Messaging, Social Networking, etc. - and we'll do the rest.
>
> Our proprietary internet filtering algorithms intelligently categorize sites so you don't have to constantly maintain a list of blocked sites.

Again, the differentiation of the legal and illegal is a complex one to marry into the same service, and we might reflect, probably should not be offered in one solution. Running the Internet Watch Foundation URL list [ref] means that illegal content related to CSEM can be effectively managed and it is unlikely that even the most freedom craving Internet libertarian would argue that this material should be access in a café WiFi hotspot. However, other forms of content blocking become more problematic, and face similar problems of over blocking.

While the introduction of Family Friend WiFi, and the resultant impact of this on other providers (i.e. they also began to filter on public WiFi) (UK Safer Internet Centre, 2015) was viewed as an online safeguarding success, perhaps with some reflection this might not be as significant an achievement as it was hailed. Admittedly, filters continued to improve, but mainly as a result of more websites becoming *white listed* – where websites that we were incorrectly blocked, could file a report with filtering providers to add them to a list which would mean that even if the filtering algorithm detects a reason to block (for example, sexual keywords in the URL or website content), the white list will override this decision and allow the site access. This, of itself, seems a curious process. A business, NGO, or individual establishing a website to provide some form of service which then, due to the filtering algorithms, ends up being blocked on either public WIFI provision or home filtering (both use similar technology and in a number of cases share the same lists). The provider therefore needs to make a report to each filtering company to ask for their (entirely legal and in no way controversial) web content to be

whitelisted, and then a human moderator with investigate it and if they decide it is indeed not harmful, the website would be added to the whitelist.

Moreover, there is a more fundamental issue, and that is does filtering public WiFi actually solve a real problem? While it is unquestionable that any internet service provision should prevent access to illegal content, and this is why the IWF services are so well regarded and successful, is the goal of preventing children accessing pornography in cafes, libraries and supermarkets a problem we needed to tackle? There is a twofold "protection" measure here – firstly, to prevent children from accessing pornography online, and secondly to prevent children seeing an adult accessing pornography online. We have posed this question many times at conferences and training events, with many stakeholders in safeguarding, and we always come to the same conclusion – we do not see individuals in public places, using public WiFi to access pornography. While it would be difficult to argue that people *should* be allowed to access pornography in public space, we would suggest that all should be entitled to access sites related to sex education, gender and human rights, mental health services, or any number of other innocuous sites on an internet connection. Yet family friendly WiFI remains something that is viewed as a step forward in algorithmic child safeguarding, even if the problem it is tackling has little evidence of existing.

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.

> The UK has established a reputation for global leadership in advancing shared efforts to improve online safety. Tackling harmful content and activity online is one part of the UK's wider ambition to develop rules and norms for the internet, including protecting personal data, supporting competition in digital markets and promoting responsible digital design.

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*'. Harking back to John Perry Barlow's manifesto, is it really the UK government's place to develop rules and norms for the internet? Of course, we would expect them to provide the legislation to manage behaviours that might be facilitated online that affect their citizens, they surely cannot define *norms* for a global technology platform?

The reason we explore it here is because we can see, from David Cameron's speech, the Online Harms white paper and the draft Online Safety Bill, that the focus remains one where technology needs to provide the solutions to these *technological problems*. And in the adult safeguarding examples we presented earlier in this chapter, we can see, again, how technology is viewed as the potential solution to supporting those at potential risk of harm online. As this ideology has progressed, we see many examples of *technological determinism* (see Matthewman, 2011) in the view that technology could tackle all manner of online social issues, centring around technology companies providing *solutions* to ensure children are safe from the variety of risks associated with going online. For example, in recent years we have had a number of calls, such as:

- A senior government minister calling for algorithms to be installed onto children's mobile phones to detect indecent images and prevent them from being

sent (House of Common Science and Technology Committee, 2017). (It should be noted that this statement is actually a useful proposal with which to deconstruct arguments around image recognition being used for the automatic detection of indecent images and therefore is discussed in far greater detail in chapter 5).

- Legislation to impose age verification technology on anyone wishing to access pornography from a UK based device (House of Common Science and Technology Committee, 2017).

- Calls to extend age verification onto social media sites to ensure no-one under 13 can access these services and for social media companies to ensure children cannot access their services for more than two hours per day (Helm and Rawnsely, 2018).

- Calls for social media companies to stop the live streaming of terrorist activities (BBC News, 2018).

- Calls for social media companies to prevent the posting of “anti-vax” materials (Mohdin, 2019).

Yet for those of us with a knowledge of the capabilities of code, we have known for a long time that technology can only ever been a tool to support to broader social context from these issues. Again the concept of *affordances* and Hutchby (2001b) is helpful to our thinking here:

There are some things that digital technology is very good at in this area. It can:

- Reporting routes and responsive, and transparent, take downs

- Warnings around content based upon keyword analysis and image comparison

- Pre-screening of some content that is easily identifiable as it has been previously identified as harmful or upsetting

- Monitoring network access and raising alerts using rule-based systems, for example, on a known website that provides access to harmful content
- The means to block abusers
- Interpreting new data based upon its similarity to previous data it has been shown.

However, there are other things that technology is far less good at:

- Inference of context of textual content
- Identification of content outside of clearly defined heuristics
- Image processing in a broad and subjective context (for example “indecency”)
- Subjective interpretation of meaning and nuance in textual data

The culmination of this policy direction has been the publication of the draft Online Safety Bill 2021 (UK Government 2021a) This was hailed by Oliver Dowden, Secretary of State for Culture, Media, Sport and Digital who said (UK Government 2021b):

> Today the UK shows global leadership with our ground-breaking laws to usher in a new age of accountability for tech and bring fairness and accountability to the online world.
>
> We will protect children on the internet, crack down on racist abuse on social media and through new measures to safeguard our liberties, create a truly democratic digital age.

The Home Secretary Priti Patel, in the same press release, said:

> This new legislation will force tech companies to report online child abuse on their platforms, giving our law enforcement agencies the evidence they need to bring these offenders to justice.
>
> Ruthless criminals who defraud millions of people and sick individuals who exploit the most vulnerable in our society cannot be allowed to operate unimpeded, and we are unapologetic in going after them.
>
> It's time for tech companies to be held to account and to protect the British people from harm. If they fail to do so, they will face penalties.

The focus remains one of expect those providing online services to ensure safety upon them, an assumption that technology can provide the answer and it the providers do not, they will be held accountable. While, at the time of writing, the bill is in draft form, and it would not be a useful exercise to have a detailed exploration of a piece of legislation that is, as stated by the Home Secretary, more about the accountability of technology companies than a broad piece of safeguarding legislation, it is worth reflecting upon this continuing the trajectory of technology solutions to technologically facilitated issues. It defines a wide ranging set of powers for a regulator (OFCOM) over technology providers, to expect them to show evidence of risk assessments to demonstrate they have thought about the potential harms that might manifest on their platforms, expecting providers to implement "safety" technologies such as monitoring and age verification, defining responsibility of platforms to manage illegal content that might be posted, but also what is defined as *legal but harmful* in the eyes of the regulator. Furthermore, it provides the government with powers to prevent app stores from carrying services that do not comply with the law, and to control access to ancillary services such as payment providers and advertisers.

The efficacy, or even implementability, of this legislation remains to be seen and could fill a separate text. For the aims of this book, however, we will pass one further observation. Within the 145 page there is far less mention of education, which is only referred to twice, in a section related to public awareness campaigns by the regulator. The responsibility of the service providers to *do more* and to expect technological solutions to what are essentially technological facilitated social problems is rife in the online safeguarding space, and can frequently cause tension between the technology providers and the policy makers. One of the fundamental points we make no apology for repeating is that technology cannot be the solution to online safeguarding.

As we have already discussed, there is a risk in our rush to safeguarding and protect everyone from the "darkest corners of the internet" there is a risk we adopt approaches that do not consider individual's rights and, in some cases, erode them. There is no piece of legislation that says that safeguarding trumps privacy. The Data Protection Act 2018 (UK Government 2018) lays down some provision for safeguarding exceptions (in Schedule 8 of the legislation), but they are limited and still very mindful of individual's data protection rights. We would argue that there is a lack of understanding *in* the stakeholder space because that is a lack of understanding *of* the stakeholder space itself (Phippen and Bond 2019). We defined a stakeholder model for online child protection (Bond and Phippen 2019), and reproduced below, which is of itself an adaptation of the seminal work of Bronfenbrenner (1979) and his ecological framework of child development. Brofenbrenner proposed an ecosystem of interconnections that facilitate the development of the child, and highlighted the different, and equally important, roles players in the system have. The important thing about Bronfenbrenner's work is that it clearly showed that there is no one independent entity that ensures positive development of the child. It is cooperative systems and the interactions between them that result in healthy development. Perhaps most importantly in his model was the importance of mesosystems – the interactions between the different players in child development.

Undoubtedly, if we are to view the draft Online Safety Bill as the leading edge of online safeguarding law in the UK, this is something we have lost sight of in this area. By adapting this ecosystem for online safety, we can see both the breadth of stakeholder responsibilities for safeguarding, and how the stakeholders interact.

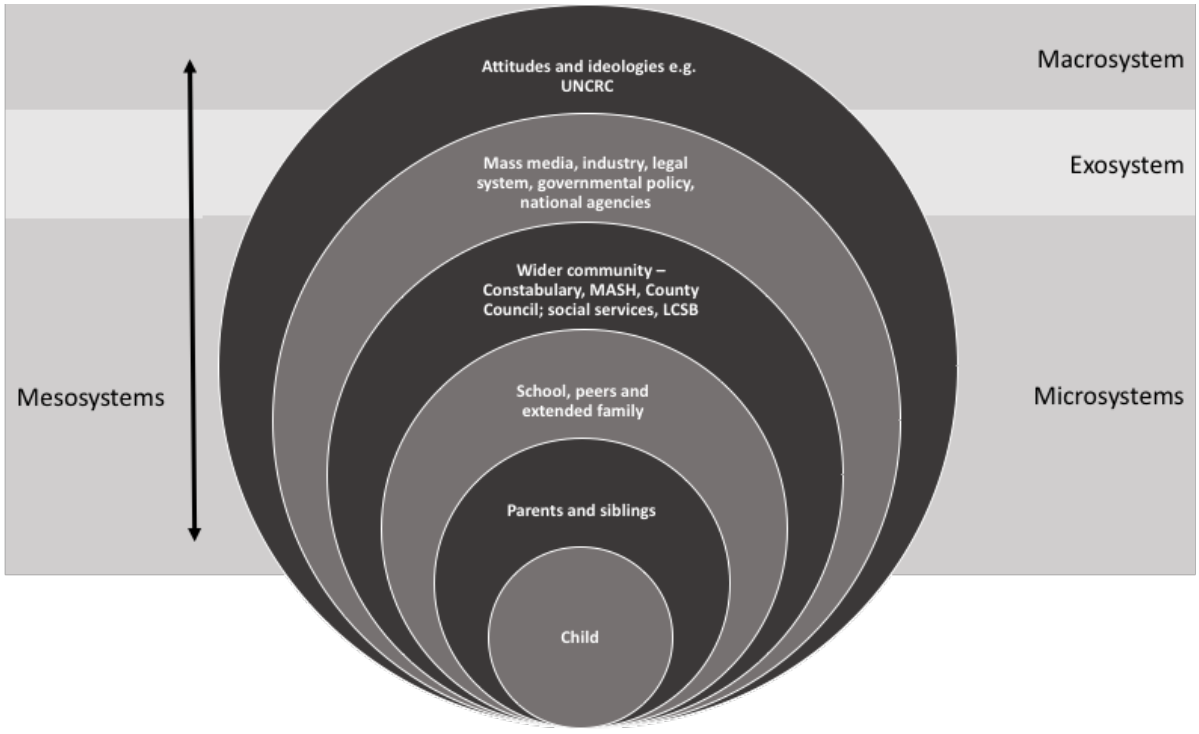


*Figure 1 – A stakeholder model for child online safety*

The value of the model is that is shows the many different stakeholders in online safeguarding, and shows the importance of interactions (mesosystems) between then, as well as the distance a given stakeholder is from the child we wish to safeguard. There are many microsystems around the child, with whom the child directly interacts with, before we even approach the place of technology provides in this safeguarding model. However, the focus of the vast majority of liability in legislation lies in an aspect of the Exosystem – industry. This focus neglects are great many stakeholders that have a role to play in safeguarding, and fails to knowledge the contribution they could, and should, make.

Within this model we defined the UN Convention on the Rights of the *Child (1989)* as the fundamental macrosystem around while the entire stakeholder space in enveloped. This should be any policy maker's go-to for the development of new resources, technologies, policy or legislation. Yet this seems to be the most neglected, and often ignore, aspect of online child safeguarding. Arguably, it is sometimes viewed as a barrier for solutions, rather than the foundation of any legislative or policy development.

## Where Are We Going?

In this chapter we have started to explore the influence of the joint Court of Protection judgements Re A EWCOP 2, 2019) and Re B EWCOP 3, 2019 ], and the subsequent ruling on the appeal against the Re B judgment EWCA Civ 913, 2019) on the world of adult safeguarding, and argued that while it is admirable that Cobb J decided to explore the child online safeguarding world in order to develop his judgements, there is a risk that building upon this foundation could end up repeating the same mistakes of this area. We will return to the adult safeguarding world in the next chapter, where we will pick up on the Cobb J judgements, the tests he defines within them, and the subsequent legacy against the MCA.