The Future of eXtended Reality Technologies, and Implications for Online Child Sexual Exploitation and Abuse

MANCHESTER
1824
The University of Manchester

The Future of eXtended Reality Technologies, and Implications for Online Child Sexual Exploitation and Abuse

Contents

Authors: Professor Stephen Pettifer, Professor Emma Barrett, Dr James Marsh, Ms Kathryn Hill, Dr Polly Turner, Dr Sandra Flynn.

This research was commissioned and funded by GCHQ to inform their understanding of the future technologies that may be used in abuse and exploitation of children. However, the views expressed are solely those of the authors. Please direct any enquiries to steve.pettifer@manchester.ac.uk and emma.barrett@manchester.ac.uk

The research and analysis for this report was largely carried out in 2019 and 2020. In early 2022, we carried out a light pre-publication update to reflect recent developments in consumer use of XR technologies.

Executive summary

This report summarises multi-disciplinary research on online child sexual exploitation and abuse (OCSEA) in the context of the development of immersive 'eXtended Reality' (XR) technologies, including Augmented Reality (AR) and Virtual Reality (VR). The project brought together expertise from computer science, psychology, and criminology. See Appendix 2 for details of our methodology and limitations.

Our purpose is to address the following questions:

- How could offenders use XR to provide new and enhance existing opportunities to access, exploit and abuse children?
- How could XR be used by offenders for the consumption of Child Sexual Exploitation and Abuse (CSEA) material?
- How could XR CSEA lead to harm to children, directly and indirectly?
- What is the future development trajectory of XR technologies? How will this influence their attractiveness to offenders?

Section 1: OCSEA offenders and victims

We summarise existing research evidence (as of 2020) relating to OCSEA, examining what is currently known about victims and offenders, focusing on offender pathways, the online risks to children and the interactions between offenders and children online. We review studies from the past 15 years (up to 2020) which examine image offending behaviour. There is not yet a specific body of research into offender use of XR technologies.

Offenders

- OCSEA offenders come from all walks of life, with varied motivations and behavioural repertoires.
- Research evidence on the degree to which consumption of OCSEA material facilitates, exacerbates, or mitigates contact (in-person) offending is mixed. Some offenders appear to follow a pathway toward increasingly extreme OCSEA material, and for some, OCSEA offending is a precursor to contact offending.
- In common with contact offenders, some OCSEA offenders hold distorted beliefs about children and sexuality. There are subtle differences in the content of the distortions between contact offenders and OSCEA offenders, with the most prevalent reported cognitive distortion for OCSEA offenders is that the virtual space is not real. Beliefs such as this allow some offenders to justify engaging in OCSEA because their actions are "not harming actual children". Yet, as with contact offences, cognitive distortions are not the only driver of offending, and more research is required to understand the links.

Online risks to children

- <u>Content risks:</u> children are potentially exposed to sexually explicit or violent material, both passively (unintentional exposure) and actively (searching for material or being directed to it by others).
- <u>Contact risks:</u> interactions in which the child is subject to online sexual solicitation (requests to engage in sexual activities, sexually explicit conversation, cybersex, or sharing explicit photos and personal information).
- <u>Conduct risks:</u> children may engage actively in risk-taking behaviours, such as purposefully accessing and/or downloading inappropriate and illegal content or sharing intimate personal information or images (e.g., sexting).
- For OCSEA offenders, online environments allow greater access to victims and more opportunities for harm with fewer direct risks to offenders.
- Compared to 'traditional' in-person abuse, OCSEA has the potential for more severe negative outcomes to victims.

Section 2: eXtended Reality technologies

eXtended reality (XR) technologies encompass a range of immersive approaches, including Augmented Reality (AR) and Virtual Reality (VR). In this section we give an overview of ways in which technology is used to create 'near reality' artificial immersive experiences and highlight the different elements of a 'virtual reality' experience.

Elements of an XR experience come together to enable the user to experience the synthetic environment as more or less real are:

- <u>Immersion</u>: the richer the immersive environment in terms of detail and number of senses being stimulated the more believable it can become.
- <u>Presence</u>: the creation of the sense of being in an immersive world, to the point that the brain ignores the encumbrances of the headset and wires and starts to react naturally and intuitively to the synthetic world as if the user were really present there.
- <u>Fidelity</u>: how precisely aspects of the virtual environment are represented.
- <u>Transference</u>: the degree to which existing real-world experience and skills can be utilised in the XR application, and correspondingly, how well experience and skills learned in the simulated environment can be transferred back to be employed in the real world.
- <u>Expressiveness</u>: the degree to which, in a social virtual environment, the technology facilitates effective communication between participants, for instance, by replicating body language (e.g., hand gestures) and facial expressions.
- <u>Technological complexity</u>: how demanding the computational hardware requirements of the XR applications are, and how effortlessly the technology solves challenges such as accurate tracking, equipment calibration, and so on.
- <u>Content and culture</u>: the range and quality of games and other XR experiences available, the social culture (sometimes called 'cyberculture') that evolves withing a shared XR environment, and the degree to which content and behaviour are policed / moderated.

Section 3. Use of technology in OCSEA

Technological developments are changing or could change the nature of OCSEA by facilitating sexual interaction in virtual environments with real children, and with representations of children. Specifically, we consider the following:

- Webcam live-streaming: live streaming of child sexual exploitation and abuse is already prevalent, mirroring adult 'camming' (streaming sexual performances via webcams and interacting with viewers).
- Virtual worlds: Sexual 'age play' and simulated abuse against child avatars has been present in online virtual worlds such as Second Life for many years. Simulated sex with child avatars may involve real children as well as adults; even if not, it may have implications for real children by reinforcing offenders' sexual interest in children and offence-related cognitive distortions.
- XR technologies: AR and VR has been taking off in the adult sex industry, with the development of immersive VR sexual games and films, the integration of haptic devices (teledildonics), and the development of adult live VR chat rooms as an extension of more traditional 'camming'. OCSEA is likely to develop along similar lines.
- Virtual depictions of children: Depictions of children in virtual environments range from cartoons to hyper-realistic images. Real children can be indirectly harmed through the legitimisation and normalisation of offence related sexual interests.
- Sex dolls and robots: Advances in robotics have facilitated the development of increasingly realistic sex dolls and robots, with the addition of movement and some degree of artificial intelligence, and programmable personalities. It is technologically feasible to develop childlike sex robots (just as childlike sex dolls have been manufactured and distributed). As with other developing technologies, sex dolls and robots can lead to indirect harm of real children through normalising of sexual interest in children.

Section 4: Future trends and implications for OCSEA

Adoption of XR technologies in CSEA contexts may be driven by:

- improvements in mobile augmented reality and internet capability (e.g., 5G)
- improvements in VR headsets (and reduced associated cost)
- increased availability of immersive video and
- growth in the adult VR industry and the immersive sex toy market.

There has been a rapid development and mainstreaming of XR platforms, and companies such as Meta (formerly Facebook) are taking steps to dominate the social XR space. XR is becoming increasingly accessible and familiar, potentially increasing risks to children, and requiring policy makers and industry to examine the regulation and moderation of immersive technologies.

Research on emerging technologies and OCSEA is in its infancy. The report has examined existing concerns and has forecasted potential future harms, but many gaps in the existing evidence base remain. It is critical that these are addressed so that harm can be reduced.

1. Online child sexual exploitation and abuse

This report summarises research from several disciplinary areas to build an understanding of online child sexual exploitation and abuse (OCSEA) in the context of the development of new immersive technologies. We focus on eXtended Reality (XR) technologies, which include Augmented Reality (AR) and Virtual Reality (VR). Our purpose is to address the following questions:

- How could offenders use XR to provide new and enhance existing opportunities to access, exploit and abuse children?
- How could XR be used by offenders for the consumption of Child Sexual Exploitation and Abuse (CSEA) material?
- How could XR CSEA lead to harm to children, directly and indirectly?
- What is the future development trajectory of XR technologies? How will this influence their attractiveness to offenders?

In this section, we provide an overview of existing published research on OCSEA, including research on offenders and victims, up to 2020.

1.1 Technology and child sexual exploitation and abuse

Technologies amplify risks posed by CSEA offenders to children, in the following ways:

- Technologies **enable consumption and production of CSEA material**, as vehicles for sharing indecent images and as platforms for accessing and interacting with children (through websites, social media, and apps)
- Technologies may influence or shape **offending behaviour** by facilitating easy access to CSEA material and opportunities for interaction with other offenders, both of which can serve to normalise sexual interests in children and offending behaviour.
- Technologies include **tools to enhance anonymity and security** (e.g., encrypted messaging, anonymous browsing, peer-to-peer networks, secure 'lockers'), thereby reducing the potential risks to an offender.

Image-based sexual abuse of children is not new: in the pre-internet era, indecent images of children (IIOC) were distributed through the mail. Images of child sexual abuse started circulating online in the early 1990s. For instance, the 'Bamse' and 'Screwdriver' bulletin boards, both operated from Denmark, distributed IIOC until they were taken down via international law enforcement action in 1992[1]. Since then, hundreds of operations have been carried out against producers, distributors, and consumers of IIOC, and yet the scale of activity remains immense.

OCSEA typically involves digital images of real children being manipulated or coerced into engaging in sexual behaviour or being sexually abused. Coercion may involve in-person physical force, or psychological manipulation, threats, and blackmail (in-person or remotely). Coercion is not always

[1] Durkin & Bryant (1995)

involved in production, however. Sometimes intimate images are created by children themselves for personal use or sharing with trusted individuals (e.g., 'sexting' with a boyfriend or girlfriend), but are subsequently shared more widely, hacked, or elicited through trickery by an offender.

Indecent images of children may be photographs, pre-recorded video, or live-streamed video with footage shared over the internet. IIOC can also include pseudo-photographs (computer-generated images that look like real photographs), tracings, drawings, cartoons, and computer-generated (synthetic) avatars of varying degrees of realism. Images do not need to be realistic to satisfy offenders: "what makes [an] image of the child important to the adult is the psychological role it plays in arousal and masturbation"[2].

IIOC are widely redistributed online, potentially in perpetuity. Images are shared, traded, and sold among wide, international networks of offenders, via peer-to-peer networks, online in 'disguised' websites, via cyberlockers[3] and on messaging apps like Telegram and WhatsApp. Rapid development in computer storage capacity, cloud computing, and file sharing platforms means that vast quantities of imagery can now be shared and stored cheaply and easily. This lowering of barriers to sharing means that offenders who might previously have only viewed IIOC can easily become distributors of such material[4].

Though a great deal of OCSEA material is still accessed via the clear internet, offenders are reportedly turning to the Dark Web where they can be more anonymous and may feel more comfortable. The National Crime Agency reports that "in 2018, 2.88 million accounts were registered globally across the most harmful CSAE dark web sites"[5]. Commercial distribution is evolving[6], with the use of anonymous cryptocurrencies like Bitcoin increasingly being used to purchase access to OCSEA material.

New and developing technologies can enhance some law enforcement capabilities and increase uncertainty for offenders around how they may be able to avoid detection. However, some advances in security and privacy technologies (including near-ubiquitous encryption) make it harder to identify and track offenders.

[2] Taylor, 2000, p. 95

[3] https://en.wikipedia.org/wiki/File_hosting_service

[4] See Steel et al., 2020, for a review of historical technology trends in OCSEA

[5] NCA, 2019, p.13. https://www.nationalcrimeagency.gov.uk/who-we-are/publications/296-national-strategic-assessment-of-serious-organised-crime-2019/file

[6] https://www.europol.europa.eu/iocta/2015/online-child-exploit.html

1.2 OCSEA offenders

This section summarises the available research in the last 15 years (up to 2020) which examines offenders use of IIOC. Research examining XR is in its infancy. Here we draw together emerging themes from research on IIOC that are likely to assist in understanding how XR might be used in OCSEA.

OCSEA offenders come from all walks of life. The majority are men, but beyond that it is not possible to define a 'typical offender'. Offenders differ in their backgrounds, motivations, patterns of behaviour, and involvement in the abuse process.

Motivations for involvement vary. Sexual motivation (i.e., sexual gratification) is common but many other motivations include coping with or displacing negative life events/experiences, profit (through commercial exploitation), and/or being part of a community (friendship and belonging)[7]. Some people have an obsessional collection tendency; for them, it is the desire to build collections of images that drives their offending (and potential associated sense of purpose and status they might not otherwise be able to achieve)[8]. An individual may experience a range of motivations linked to their OCSEA behaviour and these may adapt over time.

OCSEA offenders have different behavioural repertoires. Some view, download, and/or store IIOC but play no part in producing the images and/or have no direct contact with children (online or offline). Some pay to access IIOC, but images also circulate without payment. There is often an expectation of reciprocity: images may be swapped, or offenders given access to IIOC collections on condition that they first supply a new image.

Offenders may have **contact with children** in a variety of ways at different stages of abuse and exploitation. Historically there has been a tendency to distinguish between 'online only' abuse (viewing images, grooming) and 'contact abuse' (where an offender is physically present with their victim). However, some offenders may be involved in establishing online relationships with children (grooming) for their own personal gratification, and/or to elicit indecent images which can be shared, and/or to set up live-streamed abuse for a wider audience (which may or may not be for financial gain) – all without ever physically meeting the victims. While this is not 'contact abuse' (as traditionally understood) it is not passive fantasy-driven consumption either as it includes direct victimisation of a real child.

1.2.1 Offender pathways

This section outlines what is hypothesised about trajectories of offenders using IIOC. It is important to highlight that there is scant longitudinal evidence available. Where evidence is available, it is usually based on samples of individuals known to law enforcement. They may not be representative of the wider population of yet undetected offenders accessing IIOC.

[7] Babchishin, Hanson, & Hermann, 2011; Elliott & Beech, 2009

[8] Fortin et al, 2018; Quayle & Taylor, 2002

Script theory is one model that can assist in understanding the small number of offenders who move from viewing IIOC to physically harming children. The theory has been used to examine different criminal acts and has recently been applied to OCSEA offenders[9]. According to this model, it is hypothesised that offenders start with consumption of legal pornography, find that illegal content is readily accessible via similar search strategies, and so learn to access illegal CSEA material. Offenders gain pleasure and reinforcement from collecting and creating series or organising collections. This activity introduces offenders to peers, and via virtual socialisation they learn key words, familiarise themselves with the tools needed to find content, adopt group norms regarding IIOC, and share fantasies and reduce inhibitions[10]. Distribution of IIOC and increased contact with other collectors normalises collecting activities and facilitates learning of new technologies and sources.

A key concern is the degree to which consumption of OCSEA material facilitates, exacerbates, or mitigates contact (in-person) offending. Researchers have considered whether offenders who use OCSEA material have their urges satisfied by online/virtual material and are less likely to engage in contact offending ('catharsis') or whether use of OCSEA material is part of a pathway toward consumption of more extreme material and, eventually, contact offending. The current research base does not yet allow us to determine which (if either) is more likely to be the case.

The 'catharsis' pathway[11]: According to the catharsis theory, engaging in online child sexual exploitation and simulations of child abuse operates as a diversion for contact offending by relieving their self-identified sexual interests in children. According to this theory, engaging with online child sexual exploitation material and simulated child abuse should reduce offenders' likelihood of sexually victimising children by meeting the emotional need. However, there is no empirical evidence for this behavioural pathway. Indeed, a meta-analysis of data from the general population found those watching both non-violent and violent pornography were more likely, not less, to engage in acts of sexual aggression[12]. Determining the significance of the association is limited by the available literature, however, and more research is needed which clearly defines the content being viewed.

Pathway to consumption of more extreme material: Another theory posits that offending escalates as, over time, offenders collect more severe and increasingly abusive material to satisfy their sexual urges. One study of 40 collections[13] from convicted male CSEA offenders, showed that in nearly 40% of cases offenders collected material in which progressively younger children were depicted, and sexual abuse became increasingly more severe, a so-called 'degenerative spiral pattern'. Just under a quarter of cases had a pattern of de-escalation, with increasingly older victims and less severe abuse.

The 'degenerative spiral pattern' may reflect the changing sexual interests of the collector, indicating an evolution of material required for sexual arousal. Collectors may become habituated to IIOC

[9] Fortin, Paquette, and Dupont, 2018.
[10] Barak, 2005; Fortin et al., 2018; Quayle & Taylor, 2003
[11] Long, Alison & McManus, 2012; Riegel, 2004; Sparrow, 2017
[12] Wright, Tokunaga & Kraus, 2016
[13] More than 60,000 images in total; Fortin & Proulx, 2019

content, causing them to seek more extreme material to achieve the same level of gratification[14]. However, the content of collections may also be influenced by the availability of some types of content. Despite a desire for more extreme IIOC, an offender may be dependent on others for access to extreme CSEA material. At present, the research evidence is inconclusive.

Pathway to contact offending: It has been argued that consumption of increasingly extreme material could ultimately lead some people to contact offending, as extreme material helps offenders overcome inhibitions and normalise sexual interests in children and harmful behaviours, thus removing obstacles to contact abuse[15]. However, establishing whether and when engagement in online child sexual exploitation leads to contact sex offenses against children is challenging, requiring studies that track offending behaviour over time; arguably most of the evidence available has not allowed sufficient time for contact offending to be detected by law enforcement.

A few longitudinal studies have attempted to follow offenders who have been charged with solely OCSEA offences to establish whether they have subsequently carried out contact offences. In general, these studies found that consumption of OCSEA material was an antecedent to contact offending in a small proportion of offences. For instance, for offenders initially charged only with OCSEA offences, contact sexual offence rates are reported to range from 1% to 6% in follow-up periods of between 18-months to six years[16]. A study[17] with an average follow up period of 13 years found offenders with both contact and IIOC convictions were twice as likely to be convicted of a further sexual offence. Rates of contact offending in the IIOC only group were 2.7% compared to 14.2% in the same of study of contact and IIOC offenders. Thus, evidence for a hypothesised pathway from OCSEA to contact offending is mixed not least due to the evidence relying on detection and subsequent convictions.

1.2.2 Risk factors for different types of CSEA offending

Although a pathway to contact offending has not been established, several studies have examined dual or 'mixed' offending, in which an offender engages in both contact abuse and OCSEA, and some have attempted to identify factors that differentiate between online-only, contact-only, and dual offending. It is important to state, however, that the research outlined here is subject to bias, such as often only including those who are known to law enforcement. As such this is section is outlined to support discussions and future research efforts.

Demographic factors: Studies suggest the prototypical online offender is most likely to be male, Caucasian, single, aged in their 20s or 30s, with higher academic and occupational ability, low in antisocial traits, showing good functioning in society, but with demonstrable sexual deviancy[18].

[14] Maras & Shapiro, 2017; see also Brown & Shelling, 2019; Davis, Lennings, & Green, 2018; Houtepen, Sijtsema, & Bogaerts, 2014

[15] Fortin et al., 2018

[16] Eke, Seto, & Williams, 2011; Henshawet al., 2017; Seto & Eke, 2005; Seto & Eke, 2015; Seto, Hanson & Babchishin, 2011

[17] Elliot, Mandeville-Norden, Rakestrow-Dickens & Beech (2019).

[18] Babchishin, Hanson, & Hermann., 2011; Briggs, Simon, & Simonsen, 2011; Elliott, Beech, Mandeville-Norden & Hayes, 2009; Neutze, Seto, Schaeter, Mundt, & Beier, 2011; Henshawet al., 2017; Schulz, Bergen, Schumann, Hoyer, & Santilla, 2016.

(Note that these characteristics are not diagnostic, i.e., they cannot be used to differentiate between offenders and non-offender internet users[19]). In comparison, in-person contact offenders are significantly more likely to be older, have antisocial traits, criminal offending history, low academic and occupational ability, and history of severe mental illness. Both groups tend to engage in compulsive pornography use[20]. Dual offenders tend to show a mixture of traits. These are relatively dated studies, however with limitations such as small sample sizes by which to confidently generalise findings. Technology has advanced significantly since 2011, and there are now significantly more reports to law enforcement with respect to IIOC, and the characteristics of dual offenders may thus be less distinctive than this research suggests.

Nature of engagement: Contact-driven offenders appear to engage in shorter online relationships than online-only offenders and rapidly seek a physical meeting[21]. Dual offenders have significantly longer histories of downloading OCSEA material and possess a higher proportion of extreme material compared to online offenders[22]. One study found that the more serious the contact offence, the greater proportion of penetrative IIOC was possessed[23]. The type of images consumed appear to reflect the offender's contact sexual offences, suggesting offenders may access IIOC that match their sexual interests[24]. Studies of other sexual offenders suggest that a significant minority[25] report recreating the contents of the pornography they had viewed, including material depicting rape.

Situational factors: Regardless of an offender's urges, 'behavioural opportunism'[26] may play a part: contact and dual offenders have been found to be significantly more likely to have access to children compared to online-only offenders[27]. OCSEA offenders have been found to have greater access to the internet compared to contact offenders[28].

Early experiences: CSEA offenders are more likely to have experienced sexual victimisation compared to a general population control group, but contact offenders are more likely than non-contact offenders to have experienced childhood adversity[29]. Early sexualisation and sexual abuse has been linked to later sexual offending[30] and exposure to explicit material from a young age has been linked to the development of unrealistic and distorted sexual beliefs[31].

[19] Henshaw et al., 2017.
[20] Briggs et al., 2011
[21] Briggs et al., 2011.
[22] Babchishin et al., 2015; Long et al., 2012; Soldino, Carbonell-Vaya, & Seigfried-Spellar, 2019
[23] Long et al, 2012
[24] Houtepen et al., 2014; Owens, Eakin, Hoffer, Muirhead, & Shelton., 2016
[25] 43%, reported in Saramago, Cardoso, and Leal, 2019
[26] Long et al., 2012
[27] Babchishin et al., 2015; Long et al., 2012
[28] Babchishin et al., 2015
[29] Henshaw et al., 2017
[30] Sheehan & Sullivan, 2010
[31] Owens, Behun, Manning, & Reid, 2012

Psychological traits: Online-only offenders demonstrate greater victim empathy, lower impression management, greater self-control, and less distorted thinking compared to offline offenders[32]. These traits may be psychological barriers to contact abuse.

1.2.3 Cognitive distortions

The ways in which CSEA offenders think about abuse of children also influence their likelihood and manner of engaging in abuse[33]. Offenders who hold distorted beliefs about children and sexuality (e.g., that children desire and enjoy sex; that children are safer and more dependable partners than adults) minimise and rationalise the perpetration of harmful behaviour, which can facilitate sexually abusive contact behaviour[34].

Features of online environments can amplify cognitive distortions, reducing consideration for real-world repercussions and thus facilitating risk-taking behaviours[35], something that has been termed the **Online Disinhibition Effect**[36]. Four factors that contribute to the ODE are:

- **Anonymity:** Allows users to rationalise that their online persona is not their ‘true’ persona; they can act in ways they would not in physical life through ‘dissociation’, leading to a diminished sense of responsibility for online actions.
- **Invisibility (visual anonymity):** Online users tend to be invisible to each other, so a user does not have to worry about how they look when they post a message and they cannot see how others look when they react to the message. The lack of signs of disapproval from others can be disinhibiting. Invisibility of interlocutors can lead to depersonalisation and reduction in empathy for them.
- **Asynchronicity:** Unless engaged in a real-time (synchronous) online conversation, users do not have to deal with the immediate reaction to their online actions. This has been described as an “emotional hit and run”[37]. People can delay the costs of their actions, whilst gaining immediate gratification. The deferral of immediate reactions can increase impulsivity, weakening resilience which in turn can increase the tendency to develop paraphilic and/or addictive behaviour[38].
- **Dissociative imagination:** People can begin to believe that their online persona exists in an imaginary space, separating this from their real-world responsibilities and social norms. Any bad behaviour does not feel ‘real’ and is ‘left behind’ in the virtual world.

Whilst OCSEA offenders may display fewer cognitive distortions than contact offenders, these are still noted in the literature. Analysis of transcripts from therapy with those convicted of online offences reported distortions relating to the children in abusive images not being ‘real’, and similar

[32] Babchishin et al., 2011; Babchishin, Hanson, & VanZuylen, 2015; Elliott et al., 2009; Gottfredson & Hirschi, 1990; Henshaw et al., 2017; Lowry et al., 2019
[33] Elliott et al., 2009; Kettleborough & Median, 2017; Soldino et al., 2019
[34] DeLong, Durkin, & Hundersmarck, 2010; Hempel, Buck, Van Vugt, & Van Marle, 2015; Houtepen et al., 2014; Kettleborough & Meridian, 2017; Paquette, Longpre, & Cortoni, 2020; Soldino et al., 2019; Ward & Keenan, 1999
[35] Barak, 2005; Rimer, 2017, 2019
[36] Suler 2004, 2016
[37] Munro, 2002
[38] Montiel & Agustina, 2019

distortions were reported in research examining police interviews[39]. Such beliefs may allow offenders to justify engaging in OCSEA by believing that their actions are not harming actual children[40]. Dehumanising OCSEA victims minimises feelings of guilt and fear, enabling offenders to justify their harmful actions[41].

1.3 Online risks to children: Content, contact, conduct

Today's children are raised in a digital world surrounded by the internet and advancing technologies and used to communicating online. Technology increases children's risk of victimisation by increasing accessibility, (to children as potential victims and of potential adult offenders), opportunity, and vulnerability[42]. The sexual risks faced by children in virtual environments can be categorised as *content* risks, *contact* risks, and *conduct* risks[43].

Content risks involve a child as the recipient of harmful mass-produced content, such as sexually explicit or violent material[44]. Children can be exposed to sexualised content both passively (unintentional exposure) and actively (searching for material or being directed to it by others).

Contact risks involve interactions in which the child is, for instance, the victim of online sexual solicitation (requests to engage in sexual activities, sexually explicit conversation, cybersex, or sharing explicit photos and personal information[45]). Factors that increase the risk of online sexual solicitation are being female[46], familial dysfunction (e.g., poor relationship with parents), being gay or bisexual, and being a foreign national[47]. Children's vulnerability to being sexually victimised online can also be influenced by emotional and behavioural needs, and adverse childhood experiences[48].

Conduct risks: Normal child development involves sexual exploration and maturation, and many children engage actively in risk-taking behaviours during this time, such as purposefully accessing and/or downloading inappropriate and illegal content or sharing intimate personal information or images[49]. Such behaviour can place children at risk of online victimisation. An example is **sexting** (sending self-produced nude or semi-nude images electronically), which has been shown to raise the risk of online victimisation, including harassment, violent threats, unwanted contact, and sexual

[39] Rimer, 2017, 2019; Paquette Longpre, & Cortini, 2020

[40] Davidson & Gottschalk., 2011; Quayle & Taylor, 2003

[41] Maras & Shapiro, 2017

[42] DeMarco et al., 2017; Whittle, Hamilton-Giachritsis, Beech, & Collings, 2013

[43] Livingstone & Smith, 2014

[44] For instance, Garcia, Lopez and Jimenez (2014) found that 49% of a sample of Spanish 12 to17-year-olds had been exposed to intense sexual content on the internet. A 2005 UK survey (1,511 children aged between nine and 19 and 906 parents; Livingstone & Bober, 2005) found 57% of the children had been exposed to pornography, with 28% of the children viewing the material unintentionally.

[45] Sklenarova, Schulz, Schuhmann, Osterheider, & Neutze, 2018 conducted an online survey of more than 2,200 German adolescents aged between 14 and 17. In this sample, 23% reported being victims of online sexual solicitation over a 12-month period. 44% of those were approached by peers and 22% by adults.

[46] In a study of nearly 3000 adults who had sexually solicited minors on the internet two thirds of the sample solicited female minors, 53% solicited male minors, and 18% solicited both males and females (Schulz et al., 2016). The general characteristics of the perpetrators of online sexual solicitation of children were male, with a mean age of 24.5 years, single and employed.

[47] Agustina, 2015

[48] El Asam & Katz, 2018

[49] Garcia et al., 2014; Quayle & Cooper, 2015; Simon, Daneback, & Sevcikova, 2014

advances[50]. Children may engage in sexting because they have come to see sharing explicit material as normal, and do not perceive it as abusive behaviour (or themselves as victims of abuse)[51]. The ODE may also contribute to some children's perception of the acceptability of sexting.

Conduct risks also include bypassing age verification checks to access age-inappropriate virtual environments intended for adults. One study reported children engaging on social networking sites from an average age of nine (the usual age restriction for social media sites, such as Facebook, Twitter, and Snapchat, is 13). Eighty two percent had personal information on display to strangers, indicating a lack of awareness about personal safety in virtual environments[52].

1.4 Interactions between children and offenders

Those who are solely consumers of OCSEA material may never engage directly with a child but nevertheless contribute to harm through sustaining demand for OCSEA and, when they pay for it, financially supporting the OCSEA industry. Additionally, the literature tells us that the access of the images contributes to the sustained trauma for victims. Other OCSEA offenders do engage directly with children to produce abusive material. Much offline child abuse is carried out by people known to the child (frequently a relative) and photos and videos of this abuse are posted, shared, and traded online.

However, in online environments, strangers can initiate relationships with children from anywhere in the world and coerce and manipulate their victims into producing and sharing abusive images, without ever physically meeting the child. A survey of professionals supporting child abuse victims in the UK reported that referrals increasingly featured 'sexting' (sending sexually explicit images via messaging apps or SMS), online grooming on social networks and apps, and young people being controlled by abusers using a mobile phone[53].

Features of online environments that can increase the risks of online sexual solicitation and exploitation of children include[54]:

- **Accessibility** – wide and increasing internet access means that virtual environments are becoming more convenient and comfortable, resulting in increasing opportunities for strangers of all ages to interact. The widespread availability of OCSEA material online can support cognitive distortions by suggesting that interest and engagement in CSEA behaviour is somehow commonplace and thus 'normal' and 'acceptable'.
- **Affordability** – new and emerging technologies are relatively affordable. With increased access and more competition, high-quality products can be delivered at lower costs.

[50] Young people aged between 18 and 24 (n = 974) who reported engaging in sexting were 2.2 times more likely to be victimised online compared to those who did not (Reyns, Burek, Henson, & Fisher, 2013). In a 2014 review of fifty studies of adolescent sexting, 79% of papers reported negative outcomes including sexual objectification, violence, perpetration of sexual harassment, depression, and self-esteem (Doring, 2014).

[51] According to practitioners surveyed for *Digital Dangers*, a report from Barnardos (Palmer, 2015)

[52] Survey of 199 7- to 12-year olds; Weeden, Cooke, & McVey, 2013

[53] Ghani, 2016

[54] Barak & Fisher's "Pent-A Engine" (2001)

- **Anonymity** - individuals can explore paraphilic interests in privacy, wearing a 'virtual mask'[55]. Anonymity reduces perceived accountability for actions in the virtual world, reducing the potential for negative social evaluation for actions[56].
- **Aloneness** - offenders can work alone and unobserved in the confines of their homes. While they may socialise with like-minded others online, their views and/or sexual interests remain unchallenged in the real world, which reduces their perception of wrongdoing and legitimises their behaviour.
- **Acceptability** – behaviour that is deemed unacceptable in the real world can seem acceptable online, particularly when validated within niche CSEA offender communities.

Finally, in the virtual environment a lack of awareness of legal boundaries and an absence of visible authority can reduce perceptions of risk[57]. Supervising adults (e.g., parents, teachers) may be less competent than children at navigating virtual spaces; inadequate supervision can increase children's likelihood of victimisation[58].

1.4.1 Finding children online

Children can be sexually groomed on social networking sites, gaming platforms, mobile phones, or using interactive technology such as webcams[59], including the increasing number of live chat apps. Any place children are active online is an attractive target for CSEA offenders[60].

The most common strategy for locating potential victims for sexual exploitation has been chatrooms created for adolescents, where multiple victims can be targeted at once[61]. When approaching potential victims, offenders may pose as other children or teenagers, or post online adverts to entice children to respond[62].

Children's self-presentation and style of communication in chatrooms can increase their vulnerability to being victimised. In one 2007 study[63], screennames indicating an age, sexually suggestive names or mentioning sex online, and appearing needy or willing to engage in sexual conversation were factors deemed attractive by offenders in chatrooms.

[55] Agustina, 2015

[56] Lowry et al., 2019; Turley, 2012

[57] Barak, 2005; Montiel & Agustina, 2019

[58] Agustina, 2015

[59] Martellozzo, 2017

[60] US National Centre for Missing and Exploited Children (NCMEC), 2018

[61] Arntfield, 2015; Davidson & Gottschalk, 2011; Malesky, 2007; Wolak, Finkelhor, Mitchell, & Ybarra, 2010

[62] In theory, a more sophisticated general approach to identify vulnerable individuals could be to use standard pseudo-anonymous advertising profiles (associating with web browsers and mobile apps with their user's activities) to target a combination of demographic, age and interest characteristics on a platform like Facebook. For example, offering a particular free in-game item to only to those with specific demographic profiles could act as a vulnerability indicator within a game, but not be evident to the child. Note that as far as we are aware this is a hypothetical possibility rather than a proven technique.

[63] n = 31; Malesky, 2007

1.4.2 Manipulative grooming techniques

Offenders may obtain IIOC as part of a process that involves forming a relationship with the victim and gaining their trust, then testing the child's reaction to the idea of sex between adults and children[64]. The offender may secure IIOC by offering inducements (e.g., money, gifts or 'likes'), offering images in exchange (invoking reciprocity) or simply asking for them. The relationship may become increasingly coercive as the offender uses those images to blackmail the child into producing more and more explicit material. Offenders may alternate between strategies, revising behavioural strategies as required to meet their goal[65].

Research by the US National Centre for Missing and Exploited Children (NCMEC) and others have identified a wide repertoire of common techniques, or grooming methods, used to manipulate and coerce children. These include:

- Developing rapport, including through complimenting/praising the child, showing apparent care /empathy, talking about 'shared' interests, 'liking'/commenting on children's online posts.
- Offering or sending unprompted sexually explicit images of themselves.
- Engaging the child in sexual conversation/role-play.
- Posing as someone a child might be less wary of such as a younger adult or child, a female, a modelling agent, or someone known to the child (e.g., friend, relative).
- Promising gifts, for instance, money, gift cards, or illicit substances like alcohol, drugs, cigarettes.
- Threatening to physically hurt or sexually assault the child or people close to them.
- Using multiple online identities when corresponding with the same child (e.g., blackmailing for sexual content under one identity while also posing as supportive friend or a victim of the same offender).
- Recording/capturing images of the child without their agreement or even their knowledge, or saving sexually explicit conversations, and then blackmailing them.
- Threatening to take their own life or self-harm if the child does not provide sexual content[66].

Tactics employed by groomers differ in style, duration, and intensity, often reflecting the offender's motivations and personality[67]. Studies with victims reveal tactics including "manipulation, deception, regular contact, secrecy, sexualisation, kindness, flattery, erratic temperament, and simultaneous grooming of those around the victim"[68]. Similar techniques have also been reported in wider literature[69].

Offenders may also engage in activities to **manage risk**, for instance, ensuring the child is not an adult decoy running a sting operation (e.g., by requesting a photo), gathering information that

[64] Black, Wollis, Woodworth, & Hancock, 2015; Broome, Izura, & Lorenzo-Dus2018; Kloess et al., 2017; 2019; Marcum, 2007

[65] Elliott, 2017

[66] Adapted from NCMEC 2018.

[67] Whittle et al. 2013

[68] Whittle, Hamilton-Giachritsis, and Beech (2014), p.404.

[69] Acar, 2016; Broome et al., 2018; De Santisteban, Del Hoyo, Alcazar-Corcoles, & Gamez-Guadix, 2018; Fortin et al., 2018; Kopecky, 2017; Quayle & Taylor, 2001; Whittle et al., 2013; Winters, Kaylor, & Jeglic, 2017

enables them to assess the likelihood of being detected, such as finding out where the child's computer is being used or when their guardians are out, and exploring whether the child would tell anyone if they were being abused.

Once a level of shared trust is established sexual topics are introduced into the conversation and intimacy is intensified[70]. At this stage conversations may be moved to more private mediums (e.g., instant messaging, email) and involve more sexualised content, including sexual behaviour, chat, and fantasy rehearsal[71]. Conversational patterns differ at this stage of grooming depending on the offender; gentle pressure may be applied to test the child's boundaries, or explicit descriptions of sexual activities may be introduced.

1.5 The impact of OCSEA on victims

Scholarly research on the impact on victims of online sexual exploitation and abuse is somewhat sparse (although increasing in recent years). One reason is that it is a relatively new phenomenon (although as we saw earlier, creation and distribution of IIOC has been going on in some forms since the internet was created). Another is that there are many ethical and practical barriers for academics who wish to engage victims in research[72]. A further reason is that finding victims and survivors can be challenging. Abusers rarely identify their victims in IIOC, and victims are often impossible for the police or charities to identify and trace. Many victims may be unaware that indecent images of them are circulating online[73].

The impact of 'conventional' offline child sexual abuse is well-understood. It can be deeply traumatising, with victims suffering a range of negative psychological and emotional impacts including fear, shame, anger, anxiety, and posttraumatic stress disorder and may engage in self-destructive behaviours[74].

Harms suffered by victims of OCSEA may be even greater, with evidence that technology exacerbates harm[75]. Some of the reasons for this are set out in Table 1 below.

Victims of online sexual exploitation can experience emotional and psychological impacts, including feelings of shame, guilt, and disgust[76]. Victims can blame themselves for what has happened, distorting their perceptions of self-worth and self-concept[77]. Harm caused to the victim is ongoing, as anything shared online is likely to have a permanent record, and some victims report this being even more harmful than the actual abuse[78]. This permanence results in repeated infringement of the child's privacy and dignity in a cycle of re-traumatisation. This can impact later life by affecting careers, reputations, and relationships, and victims fear being recognised from their images[79]. Some clinical practitioners working with survivors report that victims describe the experience of abuse to

[70] Acar, 2016
[71] Kloess et al., 2017
[72] Whittle et al., 2013
[73] Ost & Gillespie, 2019
[74] Cripps & Stermac, 2018; Martin, 2015; Ramiro et al., 2019
[75] Ost, 2016
[76] Cheung, 2012
[77] Martin, 2015
[78] Ost, 2016
[79] Martin, 2014, 2015

be minor in comparison to the impact of the images being online[80]. Recorded abuse can intrude on physical integrity, humiliate the victim, and diminish privacy and autonomy[81]. Coercion and online sexual harassment are also associated with increase substance misuse (including alcohol and drugs), anger and diminished relationships with parents[82].

The use of digital technology by an offender has been found to lead to more severe physical outcomes for the victim, with one study reporting the digital component of CSEA being significantly associated with more severe forms of abusive acts[83]. In another study, victims of sexual abuse with digital component were two times more likely to be exposed to a penetrative form of sexual abuse, three times more likely to be exposed to recurrent sexual abuse, and three times more likely to be sexually abused by multiple offenders[84].

[80] Martin, 2014
[81] Ost, 2016
[82] Cripps & Stermac, 2018
[83] Say, Babadagi, Karabekiroglu, Yuca, & Akbas, 2015
[84] Cripps & Stermac, 2018

Table 1: Reasons why technology exacerbates harm for victims of OCSEA

Reason	**Explanation**	**Victim's Account**
Permanence and lack of control over distribution	It is all but impossible to remove specific IIOC completely from the internet. As a result, images may circulate for many years, potentially for the rest of the victim's life. The victim can do nothing about this.	"I have been told that my pictures are the most popular on the internet. How can so many people delight in the horrible things that happened to me? I know that these pictures will never end and that my virtual abuse will go on forever." (Victim quoted in Martin 2015)
Abuse may occur without the adult having physical contact with the child	Victims are often 'directed' to abuse themselves by adults who are either physically present but behind a camera or watching live streamed abuse and directing it remotely via chat or webcam functions. This can make a victim feel shame at the thought they were somehow responsible for their own abuse.	"My father never touched me, he always directed me, he was always behind the camera, so I always thought it's not his fault, I could never go to the police or social workers because whenever I heard about sexual offending it was the adult touching the child so I always thought therefore I am the perpetrator and it was not my father." (Victim quoted in Leonard, 2010)
'Self-generated' images	An increasing number of IIOC are 'self-generated', in that the child has taken photographs or videos believing them to be private, but they are later shared widely. This can make a victim feel shame at the thought they were somehow responsible for their own abuse.	"I feel like I can't look at myself as a good person because of everything that happened. Of course, I'm going to blame myself because I put myself in lots of these situations…" (Victim quoted in Hamilton-Giachritsis et al., 2017)
More severe physical harm	Research suggests that the use of digital technology in abuse relates to more harm and severe outcomes.	

2. ‘eXtended Reality’ technologies

The term ‘extended reality’ has been used to refer to a range of different types of immersive experience. In this section, we discuss the ways in which technology is used to create ‘near reality’ artificial immersive experiences and highlight the different elements of a ‘virtual’ or ‘extended reality’ experience. We also highlight ways in which XR is being commercialised, and the issues that this raises in terms of the availability of undesirable or illegal content.

2.1 Virtual, augmented, and mixed (‘eXtended’) reality

The term **‘virtual reality’ (VR)** refers to a believable artificially mediated experience. The form these experiences take varies widely but at their core relies on simulating a three-dimensional world and presenting it to a participant’s senses, such that their brains process and reason about these sensory inputs in a similar manner to how they experience the real physical world. The more effectively this is carried out, the better our familiarity of the real world can be used to understand what is presented within the virtual environment, and the better experience gained in a believable virtual world can be transferred back to real world. (This is clearly important in training simulations for pilots, for example.)

‘Augmented reality’ (AR) is similar to ‘virtual reality’ but instead of attempting to block out the real world, it combines a believable synthetically generated 3D environment with the physical world around the participant. Synthetic objects are not just overlaid on the screen in two dimensions but oriented and located so that they appear to be part of the physical environment and move accordingly as the viewpoint changes. Various augmented reality technologies exist for achieving this, such as overlaying computer-generated imagery on a view of the real world inside a headset using mirrors, prisms or translucent screens; combining the 3D imagery with a video feed of the real world within a headset; or simply using the video camera on a mobile phone or tablet computer and combining the video feed with synthetically generated 3D objects before displaying it.

One of the challenges of augmented reality is to track how the view of the real world is changing as the user moves around in order to update the computer-generated imagery. Much of the research in this area is trying to improve the understanding of the relationships of physical objects in the scene so synthetic imagery can pass behind or otherwise interact with them.

The most sophisticated Augmented reality headsets, such as Microsoft’s HoloLens 2, have largely been limited to industry use due to the cost and specialist nature of current applications.

One way to think about this technology is that virtual reality is just one end of a continuum of experience stretching from the real physical world to a completely believable synthetic world (only achievable in science fiction). Augmented reality exists in between these extremes closer to the real-world end and practical virtual reality towards the entirely synthetic end. A subtle nuance is that even virtual reality relies on the user perceiving real-world physical objects to achieve its effects (such as headsets, screens, audio devices and so on).

2.2 Elements of an extended reality experience

2.2.1 Immersion

Long ago movie companies understood that using a large screen, dimming lights, blocking out external noise and using powerful surround sound enhances the experience and believability of films in comparison to watching on a small television at home.

When technology is used to block out contradictory sensations and present a range of consistent synthetically generated stimuli the experience becomes ‘immersive’. In general, the richer the immersive environment in terms of detail and number of senses being stimulated the more believable it can become, though it is important that these stimuli are plausible and consistent with our expectations of the world. Generally, sight and sound are considered essential within a virtual environment, but touch (haptics) can be very effective, especially for providing feedback when interacting with virtual objects. There have even been experiments involving virtual smells and tastes[85].

There are many **technical challenges** with the equipment currently used to achieve immersion. If, for example, the sensory information about movement from the vestibular system in the ears contradicts what is being observed with the eyes it can cause motion sickness, much like being on board a ship in rolling waves without a view of the horizon. Similarly, when viewing a stereoscopic representation of a 3D scene on a screen (either inside a VR headset or on a 3D display) there is a conflict between accommodation (focussing of the eyes’ lenses through changing shape) necessary to focus on the physical screen and the degree of vergence (inward horizontal rotation of the eyes) necessary to fix on the object. Our brains automatically link the two via the ‘accommodation-convergence reflex’ and when the usual relationship between them breaks down it leads to eye strain and fatigue.

Through evolution our brains have become good at detecting unexpected or unusual behaviour. If, for example, a sound doesn’t appear to come from the same location as the object that is meant to be emitting it, we quickly notice. This is also true of other technical glitches.

2.2.2 Presence

It is important to design a virtual reality experience carefully to avoid technical issues that make the artificial nature of the virtual environment apparent. When this is successful the brain will start to ignore the encumbrances of the heavy headset and wires and start to react naturally and intuitively to the synthetic world as if the user were really present there. The creation of this belief in the user of being in a place elsewhere to their real physical location is called **‘telepresence’**, often referred to as simply ‘presence’. This belief is extremely fragile and any technical issues or unexpected intrusions from the physical world (such as a family pet jumping on the user) will shatter the illusion.

[85] For example, (Narumi at al. 2011)

(This is like riding a bicycle: an experienced cyclist does not consciously think about how they are using the machine but are instead considering their route, traffic, weather and so on. Should their chain break, however, they swiftly become aware of the technology.)

Sometimes people also refer to **'self-presence'** or **'body presence'**, which relates to how believable it is that you are now located in the space you are experiencing and not just observing it from a disembodied viewpoint. The interactivity of the environment is important here: i.e., how much you can influence and change things in the world, and how the world can affect you. Body presence is also fragile. Typically, in consumer VR systems only the hands are tracked via controllers or cameras on the headset. If the player can see their own arms, then there will be ambiguity about where the elbows should be depicted. Plausible positions can be guessed from the player's height and wrist position and rotation, but if this differs from their actual physical position the virtual body may no longer feel inhabited by the user. Often virtual environments just depict disconnected hands for users since even though this is clearly unrealistic it is less jarring than showing erroneously located arms.

Many VR applications rely on other characters being depicted in the environment interacting with the user. Some of these characters might be 'avatars' embodying fellow human participants, and some may be computer controlled. **'Co-presence'** is a term sometimes used to describe how much these characters are believable and have intention and intelligence. Co-presence is achieved both through the believability of the activities the characters undertake and the expressiveness of the animation. Within games, poor artificial intelligence controlling non-human characters can quickly make them seem unrealistic[86].

2.2.3 Fidelity and Coherency

Fidelity refers to how precisely aspects of the virtual environment are represented: the graphics, audio, participant movement and controller tracking, object behaviour, haptics (if using), and so on. People often assume "higher fidelity for everything is better" but finite computational power and rendering capabilities (and even the limitations of the speed of light when it comes to networking) demand careful judgement in where to focus resources.

For a strong and continuing sense of presence, though, it is essential that as the user of an immersive VR system moves their head objects appear to stay fixed in the same spatial location. In order to achieve this the hardware needs to:

- detect the head and controller movement (usually using some form of camera-based tracking combined with an inertial sensor);
- update the software model of the environment with new positions;
- update the environment model with changes received across the network from servers and co-inhabitants;
- update the behaviour of other objects in the world according to game rules and physics simulations;

[86] For examples, see https://www.wired.co.uk/article/video-games-surrealism-bethesda

- render (draw) the new view of the scene from the viewpoint of each eye individually and process environmental audio sources to produce spatialised stereo audio…

… all before waiting for the display technology in the viewing device to update and refresh. If any of these activities takes too long, then the frame won't update in time and objects will either snap between positions or appear to 'swim' around. This quickly breaks the sense of presence (which does not necessarily return quickly) and contributes to motion sickness.

Consequently, the cognitive and perceptual requirements of the application need to be considered to identify the most important features on which to 'spend' the 'resource budget', for instance:

- unimportant background object behaviour can be approximated if not central to the activity;
- graphical detail can be reduced to ensure rendering is always completed before the next frame is required;
- the number of audio sources can be reduced or merged so long as important nearby sounds can be processed to appear to come from the correct spatial locations;
- and so on.

If the user's gaze can be tracked, then their field of view can be estimated allowing fidelity to be increased in that region.

When rendering other inhabitants of the virtual world it is important to consider the impact of perception. The **'Uncanny Valley' effect**[87] derives from the shape of a graph in which the affinity or emotional comfort with a robot or virtual character increases with higher fidelity representation up until a point where it suddenly plummets to being extremely uncomfortable before rising again at extremely high levels of fidelity. Potential explanations for feelings of 'uncanniness' range from the idea that uncanny faces look 'dead' and thus increase 'mortality salience' (and thus fear of death), to the suggestion that uncanny feelings arise when our brains are uncertain as how to categorise a replica that closely resembles a real human[88]. Character movement similarly contributes an even greater effect: increasingly complex realistic movement makes even non-human characters emotionally relatable, but jerky or erroneous movement can induce suspicion, distrust, and discomfort. Both factors are important in engendering a sense of co-presence.

We might expect a shared virtual environment to provide a consistent and coherent view of the world to each of the connected users. However, the speed of light imposes a finite upper bound on how fast information can be communicated across a network, and in practice real network performance is well below this level once transmission media, routing, queueing, and switching is taken into account. The impact is that regardless of any hardware or software tricks, two remote users cannot share an instantaneous, fully synchronised view of a world. The designer will need to decide what aspects need to be consistently synchronised and build in mechanisms to prevent invalid behaviour such as two participants both believing they picked up the same object due to the delay in reception of the information about the other user's actions. Correcting this error would be

[87] Mori (2012).

[88] Other explanations include: Pathogen avoidance: hyper-realistic ('uncanny') human avatars share visual features with real people who are sick, prompting a disgust reaction; Evolutionary aesthetics: we have evolved to prefer physical attributes which signal fitness, and slight imperfections are deemed unattractive; Violation of expectation: feelings of uncanniness arise when expectations for human-ness are not matched by the replica; Mind perception: uncanniness arises when human-like replicas do not have matching human-like actions and behaviours (Wang et al., 2015)

necessary but break the user’s cognitive model of the environment. In practice a user rarely has a second frame of reference for what other users are doing and therefore has no means to realise there might be small delays or minor errors in observing their behaviour so long as connected behaviour is also delayed (such as maintaining an avatar’s lip sync with audio).

In addition to the delay in transmitting information, finite bandwidth (capacity to carry data) also has an impact on the fidelity with which remote users can be depicted. This is readily apparent with videos degrading to match available bandwidth on mobile telephones. It is even more obvious with the high data rates required to transmit immersive stereoscopic video or the detail of the activities of thousands of co-inhabitants of a VE. One way to manage this is to consider what spatial region of the video or virtual environment is critical to the user’s attention (such as through gaze tracking) and aim to maintain a higher fidelity there and reduce detail elsewhere.

2.2.4 Transference

One of the driving goals of virtual reality research over the past 50 years has been to offer a safe training environment which can be easily manipulated. This can help provide experience of unusual situations such as equipment failure onboard a passenger jet, operating in zero gravity, or maintenance operations that would have expensive consequences if performed incorrectly.

For existing real-world skills to be successfully transferred to VR it requires strong immersion and presence coupled with suitable interaction devices for performing whatever task is being simulated. (For example, it may be that simpler devices that better simulate a specific tool are more beneficial than a state-of-the-art multipurpose handheld controller that doesn’t feel or operate like the implement).

It is hard to generalise about the success of the transfer of trained skills in VR to the real world due to the diversity of scenarios and equipment used. However, in general for skills learned in VR to be useful, alongside strong immersion and presence, the task being trained also needs to be carefully analysed and mapped into the VR application. Sometimes this is known as ensuring **‘cognitive fidelity’** and considers how the stimulus-response relationship is managed such that the decision-making process in the VE agrees with the real-world task. For example, in some applications accurately simulating friction and using a haptic device might be identified as necessary to learn a delicate disassembly task whereas in another application the simulation of friction is an unnecessary processing overhead and the strict sequence of operations is more important.

Other areas in which an experience in virtual reality successfully transfers to the real-world include the treatment of anxiety disorders, including specific phobias, panic disorder, agoraphobia, social phobia and post-traumatic stress disorder. VR has proved especially beneficial at providing a mechanism for immersive exposure therapy where a patient can confront their phobia in a safe environment[89].

[89] (Wiederhold et al. 2014)

2.2.5 Expressiveness

Social virtual environments rely on facilitating effective communication between participants. Text based communication is notorious for misinterpreted emotional responses to otherwise context-free messages, and so implemented well, VR offers the opportunity for body language and intonation to play a significant role. Social VR environments are no better than video conferencing in this respect *per se* but scale better to many users and allow participants to share in an activity using objects in the environment.

As consumer VR has improved it has become standard for users to control their avatars to be able to gesture with the position of their hands: make a range of hand gestures such as pointing, 'thumbs up' and 'OK' signs; turn, bob and roll their head and automatically appear to lip sync to spoken words. This latter facility is fairly limited at present, but next generation VR headsets will include inbuilt cameras pointing at the eyes and face to track eye gaze and facial/mouth expressions.

Other forms of expressiveness include the use of video or volumetric 'holograms' to show remote users (particularly in augmented reality applications) and the ability to use prop objects and tools to communicate, such as indicating a mood by causing a cloud or sun object to hover over one's avatar's head.

2.2.6 Technological Complexity

A significant barrier to consumer VR adoption has been the demanding requirements of the computing hardware to be able to achieve the update requirements outlined in the *Fidelity and Coherency* section. Using a PC-based VR headset and controllers (such as offered by Oculus's Rift, HTC's Vive, Valve's Index, and Microsoft's Windows Mixed Reality) requires a recent high-performance PC containing a powerful processor and an expensive graphics card capable of quickly rendering the stereo view of the virtual scene at high resolution. The headset is connected to the PC with long HDMI and USB cables which the user has to be careful not to stumble over if they turn around since they cannot see them when wearing the headset.

The position and rotation of the headset and hand-held controllers is calculated by fusing data from high frequency inertial measurement units (IMUs) with some frame of reference to the local physical environment since IMUs quickly drift over time as double integration errors accumulate.

Valve and HTC have traditionally used at least two non-visible light emitting 'lighthouses' placed in fixed locations around the room that scan a pattern across the whole room. Multiple photo sensors in the headset and controller devices then interpret the timing of their sight of this pattern to calculate position and orientation to correct the IMU's drift.

Oculus's approach was to have infrared markers on the headset and controllers and to observe these with one or more cameras stationed around the room and connected to the PC with USB cables. From the pattern of the markers on the camera images the position and orientation can be observed.

Both tracking systems require power and/or USB leads which introduce more cables into the environment and makes set-up more time consuming. Occlusion is a significant issue in both approaches, such as if sitting behind a desk and lowering the controller below it thus breaking line-of-sight to the lighthouse or camera or moving a controller into an area shadowed by the body.

Set up and troubleshooting is not trivial with PC-based VR. Myriad hardware variations between users and frequent graphics card driver updates can have negative effects on previously working software. There is also a degree of calibration required by systems, particularly in order to define safe play areas and avoid tripping over or otherwise causing damage or injury from unseen physical objects like chairs and tables.

Newer VR headset models have moved to using a new tracking technique called ‘Inside Out Tracking’ or ‘Simultaneous Location And Mapping (SLAM)’. These again work by using an IMU for rapid updates to movement and orientation but then use multiple cameras on the headset to visually identify and track unique static features in the room as the headset moves to correct for drift. This has the significant advantage of simpler setup (no external cameras or lighthouses are required), lower cost, and easy set up and calibration. The cameras are generally also used to track the relative controller movement, which while simple, has limitations if the controller is moved out of sight such as behind the user. The system also requires bright illumination for the cameras to work which can lead to light bleeding into the headset reducing the immersion.

In previous attempts to make VR simpler, cheaper and therefore attractive to a larger market, Google, through their ‘Cardboard’ and ‘Daydream’ products, and Samsung, with their ‘Gear VR’ both produced a range of basic headsets containing little more than a pair of distance correcting lenses into which a user’s mobile phone was slotted. These just used the IMU in the phone to calculate orientation without taking into account movement, called **3 degrees of freedom (3DOF)** as opposed to 6 degrees of freedom (6DOF) when considering orientation and location. Since there was no frame of reference to the local environment the user has to look forward and hold a button to reset the IMU’s drift. Oculus subsequently launched the Oculus Go which contains the processing and screen functionality but is otherwise still a similar 3DOF device.

3DOF devices raise the likelihood of motion sickness due to the vestibular system contradicting what is being observed (as outlined in *2.2.1 Immersion*). These devices’ controllers (if they have them) are also 3DOF and thus can’t be moved up, down, left, right or towards or away from the body making them effectively function like laser pointers. 3DOF VR devices are most suited to passive media consumption such as watching immersive 2D and 3D 180° or 360° videos. 3DOF mobile VR is mostly obsolete now with little support for modern phones.

These simpler mobile devices have the significant advantage (in addition to cost) of a lack of much of the ‘encumbrance’ associated with VR, which has the potential to break the sense of presence, in particular the burden of bulky, heavy equipment and cables. (They are still encumbered by such things as heat build-up and headset and controller battery life.)

The ‘Oculus Quest’ standalone VR headset was released in 2019 and superseded by the ‘Oculus Quest 2’ (now rebranded as the ‘Meta Quest 2’) in 2020. These devices combine onboard processing and rendering with inside-out tracking allowing them to work untethered with minimal setup and ancillary costs. The drawback of standalone headsets is potentially high levels of heat generation within the headset and much reduced processing and rendering capabilities over standalone PCs. Quest offers a USB tethered mode of operation where processing and rendering can also be offloaded to a PC where desired, with the Quest 2 also offering experimental support for wirelessly linking to a PC over Wi-Fi.

A core feature promised by future 5G mobile networks is ‘edge computing’ which involves providing computation and storage resources located physically close to mobile users with very low communication latency. A similar opportunity to boost the power of standalone VR by offloading part of the computation and graphical workload to the network will be possible.

2.2.7 Content and Culture

Even the best VR hardware will be of little use without content in the form of games and other virtual reality experiences. What content is available on any given platform depends on barriers to publication and whether the popularity of the platform makes economic sense.

Some software platforms are entirely controlled by a single company such as **Sony’s PlayStation VR** and **Apple’s iOS mobile** platforms. To get published, games have to obey content rules and pass a review. This maintains quality and certain standards. For example, in 2019 Sony became concerned in the light of the ‘Me Too’ movement that it could become associated with Japanese titles that feature sexualized images of underage girls and changed its rules to avoid possible financial damage. The drawback of this approach is that it tends to lead to a lack of diversity in the market and makes it harder for small game producers to get started, but it does offer a route to control (at least to some extent) the use of VR for criminal activities such as online child sexual abuse.

Valve’s Steam Store, which sells games suitable for PC-based VR, on the other hand states: “we've decided that the right approach is to allow everything onto the Steam Store, except for things that we decide are illegal, or straight up trolling”[90]. As a consequence, Steam features a large number of sexually explicit VR games. For example, “Let's Play with Nanai” is a game that uses the inertial sensor in a mobile phone strapped to a sex doll to detect its movement and cause the character in the virtual world to react to thrusting.

Meta has its own curated store which is built into their VR platform. (This was formerly called the **‘Oculus Store’**; as part of the rebranding of ‘Facebook Inc.’ to ‘Meta’ the ‘Oculus’ brand was dropped, but it is still common to see the ‘Oculus’ name used online and by users). They have strict content guidelines but varying quality guidelines according to device. The Quest headsets have have more tightly applied criteria which aims to address criticism of game quality on previous headsets. The Quests' software runs on a modified Android system and allows ‘sideloading’ software by plugging the headset into a PC with a USB cable. This has led to a popular alternative store, **‘Sidequest’**, to emerge, containing incomplete works in progress and less polished games along with applications that fail to follow Meta’s rules. Sidequest appears to be fairly benign, however other sources like https://beta.imaginevr.io contain many sexually explicit games which sail quite close to the boundaries of UK legislation featuring childlike bedrooms and avatar faces.

Multiuser VR applications also have to decide on an approach to openness within the virtual environment. For smaller companies with limited resources there is a strong incentive **to devolve**

[90] https://steamcommunity.com/games/593110/announcements/detail/1666776116200553082

moderation to users along with encouraging the creation of worlds and other content. While giving a sense of ownership of the virtual environment to the users, a risk of this approach (taken by popular applications such as VR Chat, Bigscreen Cinema and Second Life) is that hidden environments can be created, with access through invitation only, containing undesirable or illegal content.

Regardless of application policy, Meta has built a reporting system into its user interface dashboard to notify the company about abuse from other users. It offers to record and submit a video of the abuse occurring as well as the username of the people responsible should they be using an application built on Meta's own software platform.

A more difficult form of abuse to counter is where a person uses the same username or 'handle' on multiple sites, or reveals other information, which allows their real-world identity to be determined, typically known as 'doxing'. There are numerous examples of non-immersive online gaming disputes leading to physical harassment, fraudulent fast-food orders, and most seriously, 'swatting', the causing of armed police to attend a house through fake distress calls.

The Oculus headsets previously had their own account and user identity system. With the release of the PC-based Rift S (now-discontinued) and the Quest 2 it became mandatory to log in with a real Facebook identity. This automatically links to a user's 'friends' and other online activity, revealing more personal information than necessary.

3. The use of technology in OCSEA

In this section, we focus on technologies that enable production and consumption of CSEA material. We explore technological developments that are changing or could change the nature of OCSEA by facilitating sexual interaction in virtual environments with *real* children, and with *representations* of children.

The adult pornography industry has tended to lead the application of new technologies[91], and where adult pornography leads, child sexual exploitation is likely to follow. In this section, we consider webcam live streaming, virtual worlds, virtual/augmented reality technology, and robots/dolls. For each, we give an overview of each development, explain how it is being adopted elsewhere, and then highlight how it could be (or is being) used in OCSEA. Although for clarity we treat these separately in the following discussion, these various technologies are often used together.

3.1 Webcams

3.1.1 Adult use of webcams for sexual activity

Widespread adoption of stable, high speed broadband connections has fuelled the popularity of live-streaming video applications, including live sexual interactions between romantic partners, casual acquaintances and strangers. Video chat applications (e.g., Skype, FaceTime) are commonly used for private sexual interactions as part of established and casual sexual relationships[92]. 'Web-camming', performing sexual acts in an online chatroom, has become a popular form of online sex work, facilitated by adult chatrooms (such as Chaturbate, MyFreeCams, livejasmin.com, sometimes called 'Porn 2.0'). Barriers to entry are low (all that is required is a webcam and an internet connection) and for sex workers 'camming' is a safer alternative to in-person prostitution. Webcam sex workers tap into a potentially lucrative market. In public chatrooms, online sex workers may be tipped by viewers and in private chatrooms viewers pay for a private show. The 'performances' are interactive: customers can request or direct actions and communicate with the performer via keyboard, webcam or audio[93].

3.1.2 Children's use of webcams for sexual activity

Young people's use of apps that feature webcam-enabled live chat is widespread[94]. When it comes to synchronous sexual engagement and experimentation via webcam, empirical research is quite scarce with small sample sizes and little replication, meaning that it is hard to draw robust conclusions. Available data suggest that a minority of young people engage in sexual behaviour in front of a webcam or mobile phone[95], however there is limited data on this. For instance, a survey of young people in Sweden (17- to 19-year-olds) found 12% of males and 16% of females had posed naked at least once and 6% of males and 5% of females had masturbated in front of a webcam or

[91] Maras & Shapiro, 2017

[92] Koops, Dekker, & Briken, 2018

[93] Koops et al., 2018; Pezzutto, 2019; Stuart, 2017

[94] https://www.ofcom.org.uk/__data/assets/pdf_file/0023/190616/children-media-use-attitudes-2019-report.pdf

[95] Koops et al., 2018

mobile phone camera.[96] Another study reported instances of under-18s ‘camming’ in return for payment[97]. (There is more evidence of ‘sexting’ static images; for instance, in a US study of 1398 children, researchers found 1 in 5 girls and 1 in 10 boys aged 13-17 had shared self-generated nude images with each other, and 40% considered this to be normal behaviour for people of their age[98].) Live streaming of sexual behaviour by children can thus often be voluntary, albeit in the context of a trusted relationship and/or without full understanding of the negative consequences.

3.1.3 Webcams and OCSEA

Unsurprisingly, live streaming of child sexual exploitation and abuse is already prevalent. As described in 1.4.2, OCSEA offenders use webcam sexual activity as part of their repertoire of grooming and coercive techniques, for instance, to desensitise a child to the idea of sexual behaviour in front of a camera and/or using such images to blackmail a child into participating in further, potentially more extreme, sexual acts[99].

As with adult ‘camming’, live streamed OCSEA can be viewed simultaneously by multiple offenders anywhere in the world. In some cases, the child is ‘rewarded’ and encouraged with tips or gifts. Offenders may pay to direct different types of abuse. Payment in cryptocurrencies such as Bitcoin, accessing abuse material via Dark Web sites, and connecting via VPN affords consumers a degree of anonymity, and can thus lower barriers to accessing increasingly violent and extreme forms of pornography, such as ‘torture porn’ (‘hurt porn’), and ‘webcam child sex tourism’[100]. The use of webcams to perpetrate abuse via real-time video streaming makes detection difficult, since although there may be digital evidence that a video stream existed, there may not be a recording of the content making the audit trail hard to follow[101].

Scant academic research exists on OCSEA live streaming, but some understanding of the nature and scale can be gleaned from research by the Internet Watch Foundation[102]. IWF analysis of the characteristics of victims of live-streamed child sexual abuse from more than 2000 images and videos identified between August and October 2017 found:

- 96% of the children were apparently alone, typically in a home bedroom setting.
- 96% of the images featured girls.
- 98% of the children were 13 years old or younger.
- 28% were 10 years old or younger.
- 40% featured category A or B abuse[103].
- 4% of the imagery was captured using mobile-only streaming apps.
- Children often did not try to hide their identity, location, or real name.

[96] Svedin & Priebe, 2009

[97] Jonsson, Svedin & Hyden, 2014

[98] Thorn (2020).

[99] Koops et al., 2018; Shannon, 2008

[100] Koops et al., 2018

[101] Krasodomski-Jones, 2018. Note that the extent to which digital evidence can be retrieved will depend on the streaming platform, but such evidence may include metadata or other data from devices of consumers and producers.

[102] IWF, 2018

[103] https://www.iwf.org.uk/what-we-do/how-we-assess-and-remove-content/laws-and-assessment-levels

3.2 Virtual worlds

Virtual worlds are computer-based simulated environments, defined as "synchronous, persistent network of people, represented as avatars, facilitated by networked computers"[104]. The first virtual worlds were created in the 1970s[105] but have grown in sophistication and complexity. In virtual worlds, users create their own avatars, which may be 2D or 3D representations or – more recently – XR representations allowing haptic (touch) sensations. Users can interact with other users and explore the virtual world independently.

3.2.1 Virtual worlds and sexual activity

'Simulation sex' sites allow users to choose their avatar (human or non-human) and can interact with other users' avatars in virtual worlds with varying degrees of fantasy[106]. Some research suggests that virtual sex in virtual worlds differs to text-based contact through chatrooms, as the use of real voices has been found to heighten the sense of authenticity during virtual sex[107].

3.2.2 Sexual 'age play' in virtual worlds

Virtual environments such as Second Life can be sites for 'age play' (roleplaying as a different age e.g., an adult role-playing a child). A study in 2013 reported 18% of Second Life users operating child avatars[108]. They are also sites for sexual age play: simulating child sexual abuse using avatars which resemble children[109]. This raises two specific dangers for children. First, although Second Life is an adult-only environment and age restrictions aim to prevent real children from accessing these platforms, many children can circumvent these. Simulated sex with child avatars may thus involve real children as well as adults.

Second, the simulation of child sexual abuse may have implications for real children[110]. Anecdotal evidence indicates that fantasy images of child abuse are not found alone and are often found in collections alongside images of real child abuse[111]. Virtual depictions of and engagement in child abuse may reinforce offenders' paraphilic interests and legitimise inappropriate feelings towards children, allowing for the cognitive rehearsal of child sexual abuse[112].

[104] Bell, 2008
[105] Mitchell, 1995
[106] Bailey, 2016
[107] Lynch, 2010
[108] Reeves, 2013
[109] Klein, 2014; Reeves, 2018
[110] Reeves, 2013; Weedenet al., 2013; Wilson, 2009
[111] Reeves, 2013
[112] Levy, 2002; Reeves, 2012

3.3 Extended (virtual and augmented) reality (XR)

Webcam experiences offer one level of immersion; deeper levels can be achieved using virtual and augmented reality technologies. Some argue that over the next ten years XR is set to be the next 'mega technology' trend[113]. New immersive worlds are being created, enabling gaming, live experiences (e.g., sports, concerts), and social experiences. XR technologies are becoming more accessible, with broader availability and increased affordability (see section 2).

3.3.1 XR and entertainment

Mobile device-based augmented reality technologies are growing in popularity, with existing technology already being used for games, demos, and applications, such as Google Map's city walking directions. Creating such applications is becoming increasingly easy: standard application programming interfaces (APIs) in iOS and Android perform the complicated video analysis on behalf of the application. Apple has recently acquired several AR-related companies, which suggests it is working on some form of AR headset and glasses.

The connection between AR and the real environment is a significant opportunity for marketing. For instance, applications are already available that enable customers to visualise how new furniture would look in their home. An augmented 'mirror' on a tablet device helps users see how a new hairstyle or makeup design would look on them. Marketing is less obvious in other cases. For instance, Pokémon Go is a hugely popular AR game played worldwide, in which players use mobile device GPS location to locate, capture, battle and train Pokémon characters. Companies can pay to have their physical premises featured as 'PokeStops' in the game. The aim to increase the sales at businesses, including McDonalds and Starbucks, by leading (often young) players to these shops to advance in completing the game's objectives. The game earned $1.4B during 2019, representing 81% of all AR game revenue[114].

3.3.2 XR and adult sexual activity

Interactive and immersive platforms for producing and consuming sexually arousing material are becoming increasingly prevalent. Most feature sound and vision, although XR sexual experiences featuring integration with haptic devices (mimicking the sense of touch) are also available.

The level of production can be 'amateur' (e.g., recorded by anyone using body-worn devices such as GoPro cameras; known as 'gonzo pornography') which may be for private use or sharing online, right up to professional outputs from commercial pornography studios. They may feature animated characters, avatars, or 'real' people.

VR adult sites that offer pre-recorded VR pornography are proliferating[115]. Consumption may be asynchronous, with recordings viewed and shared using wearable AR technology such as Google Glass, VR headsets or smartphone VR[116]. Users can view and experience the content in 3D as if it

[113] Munster, Jakel, Clinton, & Murphy, 2015
[114] Nielsen SuperData, 2020
[115] Gaudiosi, 2016
[116] Ashton, McDonald, & Kirkman, 2019; Eggestein & Knapp, 2014

were occurring in front of them in a somewhat realistic way[117]. Live VR 'cam' sites also exist, featuring live-streamed VR pornography and operating on the same basis as webcam chat rooms (activities incentivised by tips or payment in a private room).

Customisable Simulations

While online software stores provide some level of curation and the opportunity for regulation, direct sales of software and DLC (downloadable content) have much less oversight. One example of this category of software is 'Virt-A-Mate'. This is a VR application that runs on a high-end PC driving a tethered VR headset. The combination of using 'Unity' — a modern game engine with sophisticated graphical rendering used for many commercial games — and having the processing power available to perform high quality physics simulations supports simulating realistic characters that reduce some of the 'uncanny valley' effects (see section 2.2.3).

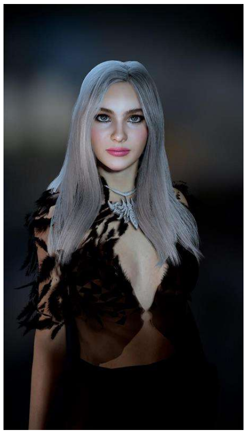

Figure 1 A character as rendered and simulated by Virt-a-Mate

Development of Virt-a-Mate started in 2017 behind a paywall, crowdfunded on Patreon. A key feature of the software is that it is a simulation construction kit with the characters being developed externally in the standard Unity game editor. The creators describe the purpose of the software as follows [118]:

> *"The goal of the project was to make advanced interactive characters using a combination of realistic joint physics, soft body physics, skin-accurate collisions, and advanced rendering techniques. The characters can come alive by capturing and storing motion capture from off-the-shelf VR equipment like the Vive or Oculus controllers and trackers. The characters will react to your movements or objects you control in a realistic manner."*
>
> *"Virt-A-Mate in its current state is meant as a creative tool for making adult content, with plenty of ready-to-use fan created content available from our active community on the official Discord server (you have the option to connect to Discord server after backing) or our official VaM Hub site."*

There are a variety of public sites, such as the Discord server described above, their 'Hub' site, and on Reddit's 'VAMscenes' subreddit[119] (35,000 members), where people can request, buy and sell user created characters. There is a clear risk that add-on characters representing children could be traded in more private forums.

[117] Brophy, 2010; Ticknor, 2019

[118] https://hub.virtamate.com/wiki/about_vam/

[119] https://old.reddit.com/r/VAMscenes/

Haptic devices

As well as enabling audio and 3D visual content, some VR systems also enable haptic content (simulating the senses of touch and motion, sometimes known as 'kinaesthetic communication' or '3D touch'). Haptic technologies can be used to control virtual objects including remote control of machines and devices (*telerobotics*), and to interact with devices that are controlled remotely. This technology has been adapted by the sex industry to enable dildos and other haptic devices to be used as masturbatory aids, mimicking the sensations of a real-world sexual experience (*teledildonics*[120]). The addition of haptic devices pairs imagery with physical action. This combines virtualised and physical elements of sexual experiences and blurs the boundary between real and virtual experiences[121].

Most existing teledildonic devices cannot currently be connected to a VR device. Instead, they connect via Bluetooth to a mobile phone app that controls their activation and frequency remotely. Some, in response to movement, can then communicate with a partner's phone via the internet and thus influence their partner's teledildonic device. In the absence of any alternative frame of reference the remote user does not know how accurately (or otherwise) their device might be reacting to what their partner is doing.

Some masturbation devices, such as the *Fleshlight Launch* (a masturbation aid for men), can synchronise movements of the device with VR videos. They do this via a phone app, synchronising the rhythm and motion of the device with action seen via the VR headset via 'script' instructions transmitted alongside some VR pornography videos. At present, syncing only works with smartphone VR headsets (the makers of Fleshlight, for example, explain "our devices are not compatible with Oculus headsets due to technicalities preventing this compatibility"[122]). Fleshlight products can, however, be used in non-sync mode at the same time as viewing VR pornography content delivered by any device.

Sexually explicit VR games with haptic elements are available on mainstream platforms such as *Steam,* designed for PC-based headsets. One such application is 'Let's Play with Nanai',[123] which uses a VR handset or mobile phone (with inertial movement sensing) to make a childlike avatar move in response to thrusting against a cushion or other surrogate object. The developer's description states: "You and an adult girl, Nanai, have a consensual sexual encounter in the form of virtual reality interactive love making." (Despite this description, the character wears Japanese school uniforms and the environments include classrooms.)

[120] Ashton et al., 2019; Maras & Shapiro, 2017

[121] Wilson, 2009

[122] https://www.kiiroo.com/products/the-fleshlight-launch-powered-by-kiiroo

[123] https://imaginevr.itch.io/lets-play-with-nanai (20,000 estimated owners using the Steam store alone; crowd funded on Patreon https://steamdb.info/app/851350/graphs/ ; https://www.patreon.com/letsplaywithnanai)

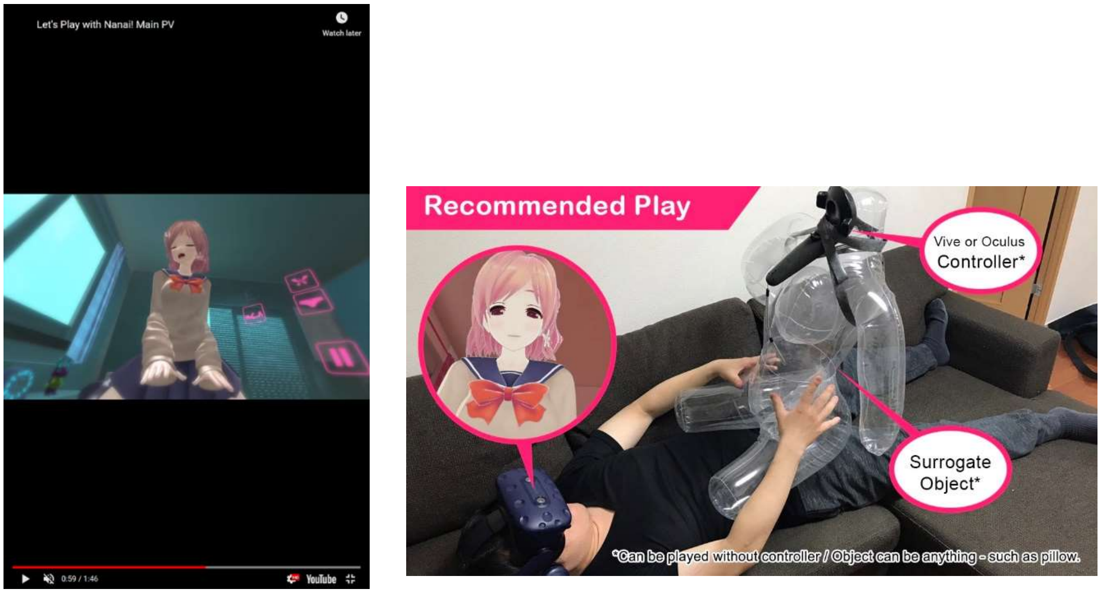
Let's Play with Nanai! Main PV
Watch later
0:59 / 1:46
YouTube
Recommended Play
Vive or Oculus Controller*
Surrogate Object*
*Can be played without controller / Object can be anything - such as pillow.

Figure 2 Sales images from 'Let's Play with Nanai!'

3.3.3 Exploitation of XR by OCSEA offenders

Research on XR OCSEA is very limited[124]. The unbounded nature of VR environments means that an increasingly diverse range of pornography is (and will become) available, including catering to paraphilic interests[125], violence and sadism. As with online environments, anonymity and fantasy role-playing are likely to facilitate disinhibited and potentially harmful behaviour. Limited research evidence suggests harassment is widespread. For example, in one study, 29% of female and 21% of male users of immersive social XR environments reported being the targets of harassment[126]. There are numerous anecdotal accounts of users experiencing abuse, harassment, and exposure to offensive content in VR environments[127].

Accessible and anonymous VR environments that allow users to experience more extreme and paraphilic material will likely normalise such behaviour[128]. Adult VR/AR pornography online communities, with forums for sharing tips and tutorials (e.g., such as that associated with Virt-A-Mate, a VR sex simulator), are likely to be mirrored by similar communities for CSEA XR, facilitating abuse and socialising the idea that sexual activity with children is acceptable.

Increasingly realistic tactile feedback will make it seem as though the user is touching the objects in the virtual scene which is likely to increase the believability and therefore enjoyment of the scene. Repeated use with CSEA material could create a conditioning effect: a strong association between

[124] Eggestein & Knapp, 2014

[125] Sexual arousal to unusual objects, situations, and/or targets, such as animals, children, corpses etc

[126] n = 110; Shriram & Schwartz, 2017. Another study reported 49% female users had experienced sexual harassment in VR (n=609; 2018 survey – see https://extendedmind.io/blog/2018/4/4/virtual-harassment-the-social-experience-of-600-regular-virtual-reality-vrusers, not peer-reviewed)

[127] E.g., "another user was performing simulated sex acts on anyone else who joined the room" https://www.facebook.com/bigscreenvr/posts/i-really-hope-you-will-give-users-more-tools-to-block-out-offensive-users-not-ju/2460239580914860/ https://www.theverge.com/2016/5/2/11569290/something-wrong-in-vr; "the virtual groping feels just as real" https://medium.com/athena-talks/my-first-virtual-reality-sexual-assault-2330410b62ee. .

[128] Brophy, 2010; Kloess, Beech, & Harkin, 2014; Martellozzo, 2017

sexualised representations of children (visual stimulus) and the user's physical sexual response. Haptic feedback may intensify this association. For some offenders, this may lead to a desire for even more extreme material to facilitate the same level of sexual gratification[129].

3.4 Virtual depictions of children

3.4.1 Cartoons and Avatars

The use of childlike avatars is popular (e.g., in Second Life virtual world, and among some internet subgroups based on Japanese cartoons[130]) but could be used for sexual purposes if the user has a sexual interest in children. Real children can be indirectly harmed through the legitimisation and normalisation of paraphilic interests among offenders, which may reduce barriers to offending against real children. Real children could also be groomed by using virtual depictions of child sexual abuse to desensitise potential victims to the concept of sex between adults and children.

3.4.2 Realistic virtual depictions of children

Realistic depictions can be difficult to differentiate from images of real children. Real images can be altered through Photoshop (a common image-editing program used to alter digital images), morphing (a way of animating a single image so it appears to change into another), or deep faking (replacing the image of one person in a video with another, in such a way as to be almost undetectable to the naked eye. Deep fake software is being used to create pornography that appears to feature celebrities, whereby a celebrity's image is merged onto the body of a porn star. It could also be used, for instance, to replace the face of one child in an indecent image with that of another child who has never been filmed in a sexualised context)[131].

A small number of studies show that men with a sexual interest in children can become aroused by such material. An ongoing 'sting' operation by the NGO Terre des Hommes (2018) involved creating a 3D model of 'Sweetie', posing as a 10-year-old Filipino girl. The image was animated (via motion capture technology) to appear as a real child on a webcam. Potential offenders interacting with the avatar found the depiction convincing[132], demonstrating how virtual depictions of children could be of interest to those with sexual interests in children.

In an experimental setting, VR has been shown to enhance sexual arousal to computer-generated IIOC. One study[133] involved exposing two groups of male participants (22 who admitted to engaging in sexual conduct with minors and 42 'non-deviant' controls) to child abuse material in auditory form (listening to stories about adult-child sexual interaction) and in VR. The VR material was a five-minute film of sexual activity involving computer-generated 3D virtual naked humans with body proportions representing either adults or prepubescent children. Measures of sexual interest (using penile plethysmography) indicated that presentation of virtual characters in immersive VR evoked

[129] Maras & Shapiro, 2017

[130] The *lolicon* and *shotacon* sub-genres of manga / anime feature sexualised "erotic-cute" depictions of girls (lolicon) and boys (shotacon) often depicted in interactions with adults; Galbraith, 2011.

[131] Photoshop: Eggestein & Knapp, 2014; morphing: Nair, 2010; deep faking: Russell, 2007

[132] In a two-month period more than 2000 individuals contacted Sweetie, resulting the identification of 1000 potential abusers from 71 countries; (Acar, 2017)

[133] Renaud et al., 2014

sexual responses, but genital arousal profiles differed for sexual offenders compared to the control group. The offender group showed significantly greater arousal to stimuli of male and female children whilst the control group showed significantly greater arousal to adult stimuli. This difference was greater in the VR condition compared to when listening to stories. Another study had similar findings with 30 child sexual abusers and 29 'non-deviant' male participants who used VR to view an animated virtual character for 90 seconds[134]. These findings imply that CSA offenders could use VR as a means of facilitating sexual gratification.

One possibility is that features of realistic VR representations of children may be off-putting to abusers. According to the 'Uncanny Valley' hypothesis (see 2.2.3), the more realistic a human virtual character, the lower the tolerance for even small imperfections in the realism of the character[135]. There is currently no research on 'Uncanny Valley' experiences and OCSEA.

3.5 Sex dolls and robots

Sex dolls are representations of humans, equivalent in size and appearance, with anatomically correct genitalia. A sex robot has been defined as "an artificial entity that is used for sexual purposes (i.e., for sexual stimulation and release)"[136]. As technology advances, sex dolls and robots have become increasingly realistic, with the addition of movement and some degree of artificial intelligence[137].

The 'relationship' with a sex doll or robot is one-way, and for some users may reinforce distorted and unrealistic expectations of real-world sexual relationships[138]. This may be exacerbated by using sex dolls depicting adults with programmable personalities[139]. For instance, 'Roxxxy' (from sex robot doll company True Companion[140]) has personalities including Frigid Farah and Young Yoko[141]. Frigid Farah is designed to reject sexual advances, and thus encourages the user to rape her, potentially normalising resistance, and the absence of reciprocity. Sex dolls and robots could promote the idea of non-consensual sex, as the user is able to overcome any resistance programmed into the doll and promote the idea that consent is not necessary.

Sex dolls can be designed to represent children, complete with accurate prepubescent anatomy and are a similar weight to a real child[142]. Possession of a childlike sex doll is not illegal in the UK, but importing, distributing, or selling a childlike sex doll is. In 2016-17, the National Crime Agency Operation SHIRAZ resulted in the seizure of 123 child sex dolls[143]. Investigation revealed that many of those who had purchased dolls also possessed indecent images of children, demonstrating a potential link between using child sex dolls and OCSEA behaviours.

[134] Renaud et al., 2012
[135] Fromberger, Meyer, Kempf, Jordan, & Muller, 2015; Mathur & Reichling, 2016; Wang, Lilienfield, & Rochat, 2015
[136] Danaher, 2017b, p.4
[137] Danaher, 2017b
[138] Maras & Shapiro, 2017
[139] Brown & Shelling, 2019; Devlin, 2018; Su, Lazar, Bardzell, & Bardzell, 2019
[140] https://en.wikipedia.org/wiki/Roxxxy, http://www.truecompaniontv.com/
[141] Maras & Shaprio, 2017
[142] Brown & Shelling, 2019
[143] Shaw, 2017

The use of child sex dolls has indirect effects on real children in several ways. Use may desensitise offenders to the notion of sexual relationships with children and normalise cognitions and behaviour regarding children and sex[144]. Users performing aggressive actions against a doll that not only lacks resistance but also provides inaccurate emotional feedback may reinforce distorted cognitions about the impact of violent sexual actions on real children[145]. Interaction with dolls may facilitate a user's transition from fantasy to real offending, and/or prompt users to seek more extreme material to fuel their interests, potentially resulting in contact offending.

Finally, the use of child sex dolls may perpetuate social isolation for some users who may not feel the need to seek, or who lack confidence in attempting, social, sexual, or romantic relationships with adults.

[144] Brown & Shelling, 2019

[145] Maras & Shapiro, 2017

4. Future trends in XR and implications for OCSEA

In this section we consider the implications of future trends in the development and use of XR technologies for OCSEA and highlight issues that will likely affect future adoption of XR in relation to OCSEA.

4.1 Future trends in AR/VR development and use

4.1.1 Increased consumer use of mobile Augmented Reality

As noted in 3.3, consumer applications for augmented reality is a fast-growing industry, and this seems set to continue. Next generation mobile devices will include dedicated hardware such as LiDAR as standard in phone cameras for determining distance to objects in a video. This will greatly improve an AR experience: with accurate depth information, synthetic objects will be able to pass behind or appear to sit on more real-world objects than simply perfectly flat ground, tables, and desks. This support is already contained in the mobile AR APIs[146].

Implications and Risks

a) Available, accessible, familiar:

Unlike AR headsets (which may cost many thousands of pounds), AR on mobile and tablet devices will become easily accessible and affordable to both offenders and victims. Such devices have the advantage also of familiarity, with a large proportion of the population having grown up with a smart phone or tablet.

b) Games designed to facilitate exploitation of children:

Even in strongly curated app stores (such as on iOS), an app review process would not be able to inspect the algorithm used by a server to deliver objectives to an individual player. With sufficient resources and expertise, motivated offenders may find it relatively straightforward to create or subvert an innocuous-looking game to attract, entrap or otherwise exploit children. An application could be designed as an outwardly normal, appealing game but with hidden functionality to manipulate and encourage specific children to go to unsafe areas, or as a method of luring potential victims to a known physical location for the perpetration of abuse. An offender could use targeted advertising (see section 1.4.1, footnote 60) or provide an in-game object to attract specific sorts of users; the object could be used to change game objectives or simply to identify the nearby location of potential victims, all without the game creator being aware of this.

On Android's Google Play store 'copycat' applications that use names and imagery very similar to popular applications are common and a poor quality 'free' game that appears similar to a commercial game may still get many installs. Malicious/abusive spin-offs of legitimate platforms could be created and be downloaded by potential victims.

[146] See, for example, https://www.apple.com/uk/augmented-reality/

c) Exploiting legitimate AR-based games to attract children for abuse

Motivating game players to venture outside and explore the real environment has obvious health benefits but may also present risks. Children could be encouraged to explore unsafe areas such as building sites or alongside busy roads, by accident or design. Indeed, there have already been reported instances of criminals using Pokémon Go to lure victims to isolated places where they are robbed[147].

In conventional online multiplayer games players often team up to defeat an enemy or solve or complete a quest. If this mechanism of gameplay is transferred to an outdoor AR game, this presents contact risks and opportunities for in-person grooming.

d) Using AR applications as part of CSEA fantasy

With improved depth information about a scene, characters could be made to explore a room, hide behind objects, sit on chairs, and seemingly interact realistically with physical objects. Offenders could exploit this by, for instance, devising 'hide and seek' games, or scenarios in which they or an avatar might sit next to a virtual representation of child (e.g., in their bedroom), visible through the screen of a tablet. Alternatively, other people or items could be introduced in a scene involving a real child to create a fantasy scenario.

Offenders could create apps that display virtual children in their own AR scene, including to create representations of abusive scenarios in their own home. Combining high-quality, freely available 3D models of children with faces from photographs it may be possible to make the child avatar look realistic, or even resemble a child known to the offender. With more advanced skills and 'deep-fake' approaches, faces could be animated in a plausible way to engage in dialogue 'inviting' abuse.

Dedicated software for this purpose is unlikely to be accepted into the curated Western mobile app stores. However, 'sideloaded' apps for Android (in much the same way as for the Oculus/Meta Quests described in section 2.2.7) and standalone PC software for mixed reality headsets could be distributed privately (e.g., on forums). The creation and distribution of such software in this manner will be difficult to police.

4.1.2 More uptake of self-contained, low-cost VR headsets and new applications

Self-contained VR headsets

The widespread adoption of 'inside-out' tracking within the industry (**see 2.2.6 Technological Complexity**) will mean newer headsets will contain outward facing cameras. Supporting mixed and augmented reality will become increasingly straightforward for the manufacturers, with more complex AR applications possible on PCs and self-contained VR headsets than 2D mobile devices.

Qualcomm, a major 'system on chip' (SOC) manufacturer for phone and VR hardware (such as the Oculus/Meta Quests, Vive Focus Plus, and HoloLens 2) released their XR2 reference headset design in 2019, illustrating hardware features of their integrated circuits that the end manufacturers could

[147] Armed robbers used Pokémon Go to target victims in Missouri; https://www.theverge.com/2016/7/10/12142434/pokemon-go-armed-robberies-missouri

use in developing future consumer hardware[148]. The Oculus/Meta Quest 2 used this SOC to boost processing and rendering performance, though the XR2 platform is capable of powering more sophisticated designs. For example, it directly supports up to seven camera feeds. A typical configuration would use four external cameras, and up to three internal cameras. Two of the external cameras would be full colour, positioned to provide typical eye separation for mixed reality applications providing a stereo video feed of the surroundings ready to be combined with 3D rendered content. Two would be optimally positioned to perform inside-out head tracking (see **2.2.6 Technological Complexity**) and to assist with depth estimation. Two of the internal cameras observe the gaze of the wearer enabling variable fidelity rendering (see **2.2.3 Fidelity and Coherency**) which devotes more of the rendering effort towards where the user is looking. In AR applications, knowing where the user is looking can be used to display contextual information over the view of the real world. The final internal camera can be used to observe mouth and facial expressions improving the expressivity of social applications. Combined with gaze tracking, avatars would exhibit better natural cues such as making eye contact and showing facial expressions (see **2.2.5 Expressiveness**).

The hardware platform provides double the CPU and graphics performance of the Quest enabling more complex graphics in standalone headsets. More complicated behaviour will be possible, such as better physical simulation of deformable objects, and improved algorithms for understanding the depth and relationships between objects in the physical world observed by the outward facing cameras.

New hand controller tracking using magnetic sensors is becoming available which allows tracking hand controllers without the problem of maintaining line-of-sight to cameras or lighthouses (see **2.2.3 Fidelity and Coherency**).

The ability of the next generation of consumer mixed reality headsets to sense the distance to physical objects in the real world will allow better interactions between virtual objects and the physical world in even more complex ways than envisaged for mobile phone and tablet AR.

VR headsets are becoming increasingly popular: 5.7 million VR headsets were sold in 2019, of which around half were Oculus (Meta) Quest headsets, despite it only being released in May 2019. Reports suggest that in 2021, headset sales reached 11.2 million (with 78% being Quest headsets)[149].

Applications

Because VR can evoke realistic responses in its users, it is a **valuable platform for training**, including the rehearsal of actual events, planning, training, and the dissemination of knowledge[150]. VR technology allows for unrestricted task repetition, 3D graphics, and can be recorded and re-watched following an activity. Practising skills in VR can lead to significant improvements in these skills in the real world[151]. For example, VR is being used in training for medicine, education, military training, arts, and entertainment[152] (see **2.2.4 Transference**).

[148] https://www.androidcentral.com/qualcomms-xr2-reference-headset-gives-us-glimpse-oculus-quest-2

[149] International Data Corporation, March 2022: https://www.idc.com/getdoc.jsp?containerId=prUS48969722

[150] Slater & Sanchez-Vives, 2016

[151] Aim, Lonjon, Hannouche, & Nizard, 2016; Bhagat, Liou, & Chang, 2016

[152] Brey, 2014

VR is being used for **exposure therapy** to help people overcome phobias and manage anxiety. Users are confronted with virtual representations of a feared situation and are supported to reduce anxiety levels to a manageable level[153].

VR is also being trialled in **pain relief**. When using immersive virtual reality, users replace perceptions of their real body with the perception of a virtual body representation[154]. When we feel embodied, the virtual representation moves according to our intentions. The manipulation of an embodied virtual body in immersive VR has been used for experimental and clinical pain relief. The pain management effect is thought to be due to the powerful distraction capacity of immersion[155].

Consumer leisure applications are proliferating rapidly, as the cost of entry to VR experience drops, making equipment (such as Meta's Quest) affordable for increasing numbers of consumers. VR applications include interactive experiences such as engaging in single- and multi-player gaming, and fitness activities (for instance, 'boxercise' in a VR gym or playing virtual table tennis). Other applications let users explore an environment, sometimes interacting with it, for instance, walking 'through' a museum, perhaps clicking on 'objects' to reveal additional information or trigger audio-visual content. Finally, users can watch film and video, and attend performances and sports matches in virtual spaces, sometimes recorded, sometimes live.

Another common activity is exploring, socialising and attending activities (such as meetings) in **virtual social worlds**. Popular platforms include AltspaceVR (owned by Microsoft), VR Chat, RecRoom, NeosVR, and Meta's Horizon Worlds. Such applications feature a combination of open spaces and open or private user-generated rooms or 'worlds'.

Implications and Risks

a) Availability and accessibility

Affordable, self-contained VR headsets will continue to grow in popularity. This is already bringing VR to a more mainstream audience than the technically inclined enthusiasts that use expensive, complex PC-based VR. Increasing numbers of children and offenders will own and use these devices regularly, and anecdotal evidence is mounting that VR social spaces are already being exploited by adults with a sexual interest in children.

Although manufacturers state that VR headsets are age-restricted (for instance Oculus and Playstation VR state they are restricted to 13+ and 12+ years old respectively), children are nevertheless regular users of VR games and social space presumably using another user's headset. The anecdotal evidence is mounting (from journalistic accounts, NGO reports, and user reviews[156]) that children access VR social chat apps and are engaging in discussions with adults in those spaces, as well as being exposed to pornography and other problematic material. From general, open social spaces, children can be encouraged to meet in private user-generated/hosted chatrooms, which

[153] Cornet & Van Gelder, 2020

[154] Hamilton-Giachritsis, Banakou, Quiroga, Giachritsis, & Slater, 2018; Matamala-Gomez et al., 2019

[155] Malloy & Milling, 2010; Matamala-Gomez et al., 2019; Triberti, Repetto, & Riva, 2014

[156] E.g., https://www.nytimes.com/2021/12/30/technology/metaverse-harassment-assaults.html https://www.theguardian.com/technology/2022/jan/09/uk-data-watchdog-seeks-talks-with-meta-over-child-protection-concerns https://www.thetimes.co.uk/article/my-journey-into-the-metaverse-already-a-home-to-sex-predators-sdkms5nd3 https://www.commonsensemedia.org/sites/default/files/featured-content/files/metaverse-white-paper.pdf

offers opportunities for offenders to groom and manipulate children using many of the same techniques discussed in section 1.

Moderation/policing of these spaces has been widely reported to be inadequate. If a child recognises an approach by another user as problematic, it can be a burdensome process to report a perpetrator. For instance, in Oculus the user has to navigate to the company website and complete a form there. In practice, most users (children or adults) will not bother or be able to report. The reporter is unlikely to know what action is taken by Meta, which is likely to decrease user willingness to report future violations. Similarly, the effectiveness of sanctions is unknown. As headsets can be shared, perpetrators of harassment may not be the registered user, and in any case the sanctions applied by Meta are unclear[157].

b) Learning new skills, overcoming inhibitions?

VR can provide a learning environment for situations which would present risk and ethical concerns in real life[158]. CSEA offenders could plan and rehearse abusive behaviour in a virtual setting before re-enacting these actions against a real child. The proven value of VR in exposure therapy indicates it could be successful in helping individuals overcome inhibitions[159]. This could encourage fantasy-driven offenders to overcome psychological barriers and fear of contact offending via engagement in rehearsal and exposure.

c) Immersion in fantasy, disinhibition

VR technology is likely to augment the online disinhibition effect (section 1.2.3), specifically through dissociative imagination (believing that an online persona exists in an imaginary space, separate from real-world responsibilities and social norms). As demonstrated in research on pain relief in VR, feeling present in the virtual environment implies psychological absence from the real world[160].

As discussed in section 1.2.3, one of the cognitive distortions held by some OCSEA offenders is the belief that activities in virtual environments are not 'real', and that actions in the virtual world do not have real-world consequences or implications[161]. Immersion in VR could amplify this belief, reducing psychological barriers to offending.

[157] Centre for Countering Digital Hate, 2022: https://www.counterhate.com/post/new-research-shows-metaverse-is-not-safe-for-kids

[158] Cornet & Van Gelder, 2020

[159] E.g., Carl et al., 2019

[160] Bailenson, 2018

[161] Paquette, Longpre & Cortoni, 2020

4.1.3 Increasing audiences for immersive videos

Streaming immersive 3D video is still a generally poor experience even for content delivered by big sites like YouTube, with the videos often pausing intermittently and degrading in quality, thereby ruining the sense of presence. Much of the current streaming infrastructure appears to have been developed for the earlier and now obsolete mobile phone-based VR headsets with more limited resolution than modern dedicated hardware.

Crisp full resolution stereo video requires between 50Mbps and 150Mbps of bandwidth to stream. Many videos available appear 'smeary' and are often not stereoscopic due either to low source quality or to the relatively poor bandwidth of much of the UK's ADSL home broadband. However, pre-downloaded immersive 3D video content played from storage on the headset or PC is crisp and compelling.

Improvements to streaming infrastructure are occurring alongside the increasing ownership of VR headsets. 5G mobile data will offer higher bandwidth than most home broadband connections in the UK along with the option to cache immersive video on 'edge servers' closer to the consumer for reduced delay and better experience.

There is already a significant commercial market for 3D immersive pornography and the relatively low cost of production means this is likely to further increase (see section 3.3.2).

Implications and Risks

Although material available to view using VR hardware on sites such as YouTube have historically been poor in quality, immersive 3D content can be downloaded to storage on the headset or PC. This material is of better quality and could mean that child sexual abuse material is more likely to be sourced from collections accumulated by offenders. An alternative would be to settle for low resolution material, without the glitches that may occur in high resolution videos. As discussed in sections 1 and 3, live-streamed abuse is a popular platform for consuming abusive material among offenders. With custom software offenders could potentially interact with the live scene being viewed in VR, pointing, gesturing, and speaking to influence the activity.

4.1.4 Availability of 3D cameras for recording immersive videos

Cameras capable of recording hemispherical and spherical videos for immersive video are becoming commonplace and affordable for the consumer. For example, at the time of writing the GoPro Max offers 2D 360° video capture for under £500 and the Vuze XR offers 3D 180° video for under £400. Several companies are promising 3D 180° webcams suitable for 'camgirls' to use for interactive live streaming pornography. Low resolution stereo 3D webcams aimed at children have been marketed in Japan for over a decade.

Figure 3 Minoru: The world's first consumer 3D webcam

With crisp stereo video requiring between 50Mbps and 150Mbps of bandwidth to stream, hosting a live streaming source at home is unlikely without a specialist connection at present. However, 5G mobile is theoretically capable of offering more than the required upload bandwidth in the future and may eventually reach 65-120Mbps.

Implications and Risks

The development and increasing affordability of 180° or 360° cameras could facilitate the live streaming of child sexual abuse to the VR headsets. The increased bandwidth offered by future 5G mobile networks will make streaming this material more generally feasible. Offenders are already able to make requests during live-streaming sexual abuse via webcam, and the presence of microphones in VR headsets could facilitate the same type of interaction.

4.1.5 Growth of the market for teledildonics and immersive sex toys

In section 3.3.2 we described how teledildonic and immersive sex toys are already being used in XR applications. The 'sex tech' industry is likely to grow significantly in the coming years[162] driven by customer demand and facilitated by the expiration in 2018 of a patent on remote controlled sex toys, which had hitherto held back the teledildonics industry.

Aside from the potential mainstream commercial market for teledildonics, there is also research interest in remote-controlled sex toys for people with disabilities (e.g., a Bluetooth-enabled device controlled via a brain-computer interface designed for people with spinal cord injury[163]).

As described in 3.3.2, at present the ability for haptic devices to be synced with a live XR performance is limited, though over time it is likely that the technical barriers will be overcome. In the medium to long-term we can expect continued development of immersive sex games (such as *Let's Play with Nanai*, section 3.3.2) that could include increasingly sophisticated teledildonic elements.

Implications and Risks

a) Reinforcing offending/risk behaviour

When imagery is synchronised with teledildonic/haptic devices, increasingly realistic tactile feedback can make it seem as though the user is touching the objects in the virtual scene which is likely to increase the believability. Repeated use with CSEA material can create a conditioning effect in the offender: a strong association between sexualised representations of children (visual stimulus) and the user's physical sexual response. Haptic feedback may intensify this association. For some offenders, this may lead to a desire for even more extreme material to facilitate the same level of sexual gratification[164].

b) New ways to harm children

Devices could be used against children as part of abuse, potentially causing physical harm, and the increased believability of the experience may increase psychological harm. Just as adult 'camming' has been mirrored by live-streamed child abuse, it is likely that OCSEA offenders will follow the same

[162] https://www.forbes.com/sites/frankicookney/2019/09/29/high-tech-sex-toys-are-a-growing-trend-and-here-are-5-of-the-best/

[163] Gomes & Wu, 2018

[164] Maras & Shapiro, 2017

route with VR. It would not be surprising if live VR chat rooms featuring child abuse, potentially using teledildonics, became available in the near future.

4.2 Virtual Reality Based Offender Treatments

Virtual reality-based therapies could offer options for intervention and treatment of offenders (see **2.2.4 Transference**). Empathy deficits are risk factors for sexual offending against children[165]. Studies show that perspective-taking in VR can increase the level of empathy felt by users towards others, include children[166].

This raises the possibility of using VR to support offender rehabilitation, with the aim of increasing victim empathy and reducing anti-social behaviours. Studies suggest that physiological responses to VR scenarios have some value in discriminating between sexual offenders from controls based on their sexual interests[167]. This indicates that VR could be paired with gaze-tracking and used to provide insight into cognitive processes, focus, and attentional states from offenders' perspectives[168].

[165] Babchishin et al., 2011; Elliott et al., 2009; Hirschtritt, Tucker, & Binder, 2019; Houtepen et al., 2014

[166] Hamilton-Giachritsis, Banakou, Quiroga, Giachritsis, & Slater, 2018; (Such effects have also been demonstrated with ethnic minority groups [Peck, Seinfeld, Aglioti, & Slater, 2013] and victims of domestic abuse [Seinfeld et al., 2018])

[167] Renaud et al., 2014

[168] Cornet & Van Gelder, 2020

4.3 Issues that will affect future development of XR and its potential for use in CSEA

4.3.1 Mainstream VR platforms and the 'Metaverse', and associated regulation and moderation challenges

Several recent developments have changed the VR social landscape, raising new challenges for regulation and moderation. In October 2021, 'Facebook Inc.' renamed itself 'Meta' and brought the word '**Metaverse'** back to media and thence public attention. The term 'Metaverse' originated in the 1992 novel, 'Snow Crash' by Neal Stephenson, which described a dystopian anarcho-capitalist world from which an immersive, multi-user, three-dimensional virtual world, the 'Metaverse', provided escape. Some of the ideas in the book, such as the unregulated, emergent culture of the Metaverse, helped influence the development of the decentralised, open culture of the nascent World Wide Web at the time.

The term 'Metaverse' was often used in 1990s VR research to describe both the ideas of moving seamlessly between independently created virtual worlds (much as you would follow links from one webpage to another), and separately, the organisation of the metaphysical rules that described the differing behaviour of the various worlds. Later the term became associated with the social online virtual worlds like 'Second Life', in particular because of the prominence of the user-created and social aspects of the world, rather than relying on an organised, game-like objective to provide interest.

What the 2021 use of the term means is less concrete. By renaming the company to 'Meta' and declaring itself to be building towards *the* 'Metaverse', Facebook attempted to claim ownership of the concept. However, it is not alone, and there will be many attempts at building differing metaverses, not all of which will be immersive. Central to many visions of the new metaverses are the use of digital currencies, with Meta announcing it wanted to develop in-world cryptocurrencies and NFTs (Non-fungible Tokens[169]) to facilitate the ownership and trading of digital spaces and artefacts[170].

Epic Games (producer of the game **Fortnite** and the widely used 'Unreal' game engine) have pursued their idea of a metaverse by introducing construction tools into Fortnite for users to build their own islands, as well has hosting events and movies within the world. They plan to eventually open up the power of their full Unreal game engine editor to enable sophisticated behaviour to be implemented in the Fortnite environment[171]. They have also expressed the desire to interoperate with other platforms. Their in-game currency is known as 'V-Bucks.'

Roblox is a popular social virtual environment rated as suitable for ages 7+ in the UK and Europe and that has 42.1 million daily users worldwide[172]. Created in 2004, Roblox has changed how it describes itself over time: as a game, an experience and now a metaverse. It hosts music and marketing events

[169] NFTs are unique cryptographic tokens that can be used to indicate ownership of some external thing — either digital, physical, or conceptual — and which can be traded or exchanged

[170] https://about.fb.com/news/2021/10/founders-letter/

[171] https://www.fastcompany.com/90741893/epic-games-ceo-tim-sweeney-talks-the-metaverse-crypto-and-antitrust

[172] https://www.theverge.com/2021/7/7/22457264/roblox-explainer-game-app-faq

and lets users create their own games and environments using the flexible programming language ‘Lua’. Much of the company’s income derives from the in-game digital currency, ‘Robux’, and from creating marketing experiences for brands, including selling branded items to customise avatars.

While Roblox has parental controls, employs AI plus human-based moderation, and prohibits sexual content, children have still found ways to circumvent these controls[173] such as using external platforms like Discord alongside Roblox to voice chat to other users free of filtering and to share links to user-created, hidden, sexually explicit, subgames known as ‘condo games.’

Facebook originally announced their attempt at a user-editable virtual world in September 2019, originally calling it ‘Facebook Horizon’ it was later renamed ‘Horizon Worlds’ as part of their overall rebranding. It was finally released in North America in December 2021. (At the time of writing there is no release date announced for the rest of the world.) Confusingly, Meta also rebranded many of their other apps to include the ‘Horizon’ name such as ‘Horizon Venues’ (a kind of immersive video player showing pre-recorded events), and ‘Horizon Workrooms’ (an immersive meeting environment). Despite the similarity in the names there are no connections between these applications and a user must exit out of one to enter another. The only monthly user figures published aggregate the ‘Horizon Worlds’ and ‘Horizon Venues’ applications together and it is likely a significant proportion of the 300,000 monthly users announced in February 2022[174] is dominated by free events in ‘Horizon Venues’. At present the environments that users can build in ‘Horizon Worlds’ and the complexity of the behaviour that can be assigned to objects is limited resulting in widespread online criticism of the experience being much below that commonly experienced within games[175]. As noted in 4.1.2, users of the Meta’s applications (including Horizons) are meant to be age-restricted, requiring a Facebook account only available to ages 13+. However, reviews[176] of ‘Horizon Worlds’ suggest many younger children are using the environment (likely by using an adult’s headset) and that there is a lack of moderation.

Many other companies have also stated they are involved in building metaverse products. Microsoft, for instance, has started adding the label to existing products from their business and gaming ranges. In addition to the technology companies with experience in social networking and gaming backgrounds, many cryptocurrency related businesses have recognised an opportunity: both from riding on the publicity surrounding the Metaverse and in finding new customers and applications for products like NFTs. Yuga Labs, for example, recently disrupted the Etherium blockchain by selling NFT ‘deeds’ to plots of ‘land’ in an as-yet unbuilt metaverse project they call ‘Otherside’[177].

Without a renewed focus on moderation from companies, it will be difficult to enforce laws and regulations within these virtual environments. A particular challenge is illustrated by Fortnite where despite a robust attempt at moderating in-game communication, children simply switch to communicating ‘out of band’ by another mechanism.

[173] https://www.fastcompany.com/90539906/sex-lies-and-video-games-inside-roblox-war-on-porn

[174] https://uploadvr.com/horizon-300000-monthly-active-users/

[175] https://www.techradar.com/uk/reviews/facebook-horizon-worlds

[176] https://www.oculus.com/experiences/quest/2532035600194083

[177] https://www.theguardian.com/technology/2022/may/02/yuga-labs-apologises-after-sale-of-virtual-land-crashes-ethereum

Should a feasible peer-to-peer virtual environment platform emerge, strong encryption and decentralised hosting would make it especially difficult to identify CSEA offenders using the platforms. Although difficult to create, peer-to-peer networks are relatively cheap to run and difficult to police, offering increased privacy and security to offenders and potentially create an environment in which problematic behaviour and law-breaking is common[178]. The development of legitimate open peer-to-peer virtual environments is likely to be motivated by opposition to Facebook's dominance and corporate attitude to privacy.

Companies like Meta will have a vested commercial interest in moderating users' behaviour to protect the company from reputational damage or further regulation. As part of committing to making Horizon a safe 'family-friendly' environment, Oculus introduced new features in 2018 to help maintain user safety. As well as creating a 'safety centre' and code of conduct, it enables users to record any experience of harassment or abuse from a first-person perspective, to be reported to the Community Operations team and subsequently be used as evidence.

This could help overcome some of the difficulties tracing digital footprints in VR, though can only apply to applications owned by Meta (and running on Meta's own servers). It will not help where a Meta VR device is being used as a client to access a cross-platform, third party operated virtual environment, such as RecRoom or VRChat. These systems use their own login mechanism and thus information about of the identity of a reported participant is located within their servers. Solving this cross-platform moderation in a privacy-centric manner will be necessary should the interoperability promised by some visions of the 'Metaverse' be realised.

Across all the platforms described here, the increasing requirement to use digital currencies and NFTs to gain status, ownership and access within virtual worlds will present an increased risk of grooming through gifting (see section 1.4.2), though as these transactions will likely be blockchain based (and therefore appear on a public ledger) they will be susceptible to forensic investigations and tracking.

Use of child-like or child avatars

Previous experience of virtual worlds has shown how CSEA offenders have exploited their functionality, including presenting sexual material using avatars with childlike appearances (e.g., in Second Life). The legal picture with respect to child/child-like avatars differs considerably across jurisdictions[179] and a detailed discussion of these is beyond the scope of this report. However, as the use of XR applications becomes more prevalent potentially resulting in an increase in incidents involving child/child-like avatars, we anticipate increasing public, law enforcement and regulatory debate around these issues. In jurisdictions where creation and/or interaction with child/child-like avatars has been criminalised, prosecutions may increase, with implications for new case law. Authorities in jurisdictions where child/child-like avatars are legal will likely face pressure to review their position. The legal situation is further muddied by large multiuser virtual environments being hosted using multiple cloud computing services that span national borders. The opaque, proprietary nature of the systems means there will be no mechanism to only block specific sub-environments.

[178] Barak, 2005

[179] Cornelius, 2011

In 2019 Facebook (now Meta) publicised their development of '*Codec Avatars*', designed to create what amount to realistic 3D deep-fake representations of real people using just a small number of photographs taken on a mobile phone. They write[180]:

> Body language is critical to our ability to communicate. That's why today we're introducing full-body Codec Avatars. While you won't find this technology in a consumer product anytime soon, we imagine a future where people will be able to create ultra-realistic avatars of themselves with just a few quick snaps of their phone cameras and animate them via their headsets. And that future will usher in a new wave of fully immersive VR.

The identification of an avatar with a real person could easily be abused to influence others without the depicted person's input or knowledge. This is explored in a recent article from the Electronic Frontier Foundation[181]:

> Hyper-realistic avatars also raise concerns about "deep fakes". Right now, deep fakes involving a synthetic video or audio "recording" may be mistaken for a real recording of the people it depicts. The unauthorized use of an avatar could also be confused with the real person it depicts. While any avatar, realistic or not, may be driven by a third party, hyper-realistic avatars, with human-like expressions and gestures, can more easily build trust. Worse, in a dystopian future, realistic avatars of people you know could be animated automatically, for advertising or influencing opinion. For example, imagine an uncannily convincing ad where hyper-realistic avatars of your friends swoon over a product, or where an avatar of your crush tells you how good you'll look in a new line of clothes. More nefariously, hyper-realistic avatars of familiar people could be used for social engineering, or to draw people down the rabbit hole of conspiracy theories and radicalization.

It is not hard to imagine this kind of technology also being abused by an offender in the manipulative grooming of children. Recognisable avatars of the child's friends could be made to engage in explicit, boundary-breaking behaviour to exert peer-pressure on the victim.

Monitoring, investigation, and enforcement

The content shown in VR contexts will be difficult to monitor. Many platforms will deliberately attempt to avoid legal responsibility by requiring users to assume responsibility for content. The social VR platform BigScreenVR's terms of service, for example, state that users "are solely responsible for your User Content" and "You assume all risks associated with use of your User Content"[182]. This platform streams videos and other software (such as conventional non-VR games) from one participant's PC to other users who experience it as if sat together in a movie theatre. The videos are not hosted on the BigScreen servers, and the video stream will not necessarily match any database fingerprints due to being reencoded for streaming at the source.

[180] https://tech.fb.com/inside-facebook-reality-labs-research-updates-and-the-future-of-social-connection/

[181] https://www.eff.org/deeplinks/2021/06/your-avatar-you-however-you-see-yourself-and-you-should-control-your-experience-0

[182] https://www.bigscreenvr.com/termsofservice (checked May 2022)

The ‘live’ experience of a three-dimensional virtual scene does not leave an informative digital footprint meaning that it is hard to establish or prove that abuse has been perpetrated in VR unless explicitly recorded at the time by a participant (such as with the Oculus/Meta abuse reporting system described in section 2.2.7). Some researchers have investigated client application logs, which in some cases show when different users enter the same virtual space. However, unlike a web browser’s on-disk history and cache, these log details are not intrinsic to the software’s functioning, but simply left in as a troubleshooting mechanism by the developers.

4.3.2 Financial issues

The effort and overall cost associated with creating large sophisticated XR experiences could naturally limit the exploitation of this technology for criminal purposes. The development of rich, immersive experiences likely to attract significant numbers of users is expensive and requires highly skilled and experienced developers. For example, the well-received[183] immersive VR game Half Life Alyx, released in March 2020, took 80 developers[184] and four years to produce around 15 hours of playable content. Not all XR experiences require this degree of realism though. As the ‘Uncanny Valley’ phenomenon described in section 2.2.3 demonstrates, in some cases providing simpler graphics and believable behaviour produces a better result for a given amount of effort. However multiuser XR platforms also require hosting the server side of the system within cloud service providers which is expensive and therefore likely to require a significant source of revenue.

For consumers, the lower cost of self-contained VR devices should see further reductions in cost over time as popularity increases and economies of scale are realised (see sections 2.2.6 and 4.1.2). Similarly, the integration of AR technology into all the major mobile platforms will mean consumers see a range of augmented reality applications appearing as standard for no additional cost. Augmented reality headsets on the other hand are likely to remain an expensive business-focused device for the near future.

4.3.3 User experience

The user experience of XR hardware is likely to continue to improve as outlined in section 2.2.6. However, issues such as motion sickness (caused by conflicting information from the human vestibular and visual systems, described in section 2.2.1) are not likely to be solved through technology alone. With prolonged exposure to VR some people adapt better than others, so software developers are increasingly offering a choice of movement paradigms for users depending on personal comfort.

Presence technologies (such as virtual reality) can cause physiological, cognitive, and emotional responses in humans in response to virtually mediated interactions, similar to responses which would be elicited by an authentic first-hand experience[185]. Temporary escapism to the virtual environment can provide stress relief.

[183] https://www.gamesindustry.biz/articles/2020-03-24-half-life-alyx-reaches-43-000-concurrent-users-on-launch-day

[184] https://uploadvr.com/half-life-alyx-developer-size

[185] Lynch, 2010

Online CSEA can result in more severe and long-lasting psychological and physical impacts on the victim compared to sexual abuse in which there is no digital element (section 1.5). The level of embodiment felt by users of VR could further heighten the consequences of this experience compared to engagement in other virtual environments. Experience of harassment in VR could feel more physically invasive than harassment in less interactive and immersive platforms, such as chatrooms. This could mean that psychological and physical implications of experiencing harassment and abuse in VR could be more severe than for earlier forms of OCSEA.

4.3.4 Social norms and socialisation

Technology gives those with a sexual interest in children a new medium to share information, explore new identities, network with like-minded individuals, and normalise their behaviour[186]. Virtual worlds can provide social interaction which reduce social isolation, allow values and culture to be shared, and validate desires[187]. The process of socialisation in virtual environments enables offenders to learn key words and techniques of sourcing sexually explicit material of children[188].

Offending communities tend to develop social norms that justify and normalise offending behaviours. Such norms will develop in XR communities and virtual worlds used by CSEA offenders. The continued development and marketing of immersive sex games that depict childlike characters could lead to a broader audience for CSEA-like material and normalise sexual attraction to children.

[186] Palmer, 2015
[187] Reeves, 2012
[188] Fortin et al., 2018

5. References

Acar, K. V. (2016). Sexual extortion of children in cyberspace. *International Journal of Cyber Criminology*, 10(2), 110-126.

Açar, K. V. (2017). Webcam child prostitution: An exploration of current and futuristic methods of detection. *International Journal of Cyber Criminology*, *11*(1), 98-109.

Aïm, F., Lonjon, G., Hannouche, D., & Nizard, R. (2016). Effectiveness of virtual reality training in orthopaedic surgery. *Arthroscopy: The Journal of Arthroscopic and Related Surgery*, *32*(1), 224-232.

Agustina, J. R. (2015). Understanding cyber victimization: Digital architectures and the disinhibition effect. *International Journal of Cyber Criminology, 9*(1), 35-54.

Arntfield, M. (2015). Towards a cybervictimology: Cyberbullying, routine activities theory, and the anti-sociality of social media. *Canadian Journal of Communication, 40*(3), 371-388.

Ashton, S., McDonald, K., & Kirkman, M. (2019). What does 'pornography' mean in the digital age? Revisiting a definition for social science researchers. *Porn Studies, 6*(2), 144-168.

Babchishin, K. M., Hanson, R., & Hermann, C. A. (2011). The characteristics of online sex offenders: A meta-analysis. *Sexual Abuse, 23*(1), 92-123.

Babchishin, K. M., Hanson, R. K., & VanZuylen, H. (2015). Online child pornography offenders are different: A meta-analysis of the characteristics of online and offline sex offenders against children. *Archives of Sexual Behavior, 44(*1), 45-66.

Bailenson, J. (2018). *Experience on demand: What virtual reality is, how it works, and what it can do*. WW Norton and Company.

Bailey, D. E. (2016) Virtual reality sex is coming soon to a headset near you. [Online] The Conversation, May 18. https://theconversation.com/virtual-reality-sex-is-coming-soon-to-a-headset-near-you-57563 [Accessed 1 March 2021]

Bailin, A., Milanaik, R., & Adesman, A. (2014). Health implications of new age technologies for adolescents: A review of the research. *Current Opinion in Pediatrics, 26*(5), 605-619.

Barak, A. (2005). Sexual harassment on the internet. *Social Science Computer Review, 23*(1), 77-92.

Barak, A., & Fisher, W. A. (2001). Toward an internet-driven, theoretically based, innovative approach to sex education. *Journal of Sex Research, 38*(4), 324-332.

Beech, A. R., Elliott, I. A., Birgden, A., & Findlater, D. (2008). The internet and child sexual offending: A criminological review. *Aggression and Violent Behavior, 13*(3), 216-228.

Bell, M. W. (2008). Toward a definition of "virtual worlds". *Journal for Virtual Worlds Research 1:1*

Bhagat, K. K., Liou, W. K., & Chang, C. Y. (2016). A cost-effective interactive 3D virtual reality system applied to military live firing training. *Virtual Reality*, *20*(2), 127-140.

Black, P. J., Wollis, M., Woodworth, M., & Hancock, J. T. (2015). A linguistic analysis of grooming strategies of online child sex offenders: Implications for our understanding of predatory sexual behavior in an increasingly computer-mediated world. *Child Abuse and Neglect, 44*, 140-149.

Brey, P. (2014). Virtual reality and computer simulation. In *Ethics and Emerging Technologies* (pp. 315-332). London, UK: Palgrave Macmillan.

Briggs, P., Simon, W. T., & Simonsen, S. (2011). An exploratory study of internet-initiated sexual offenses and the chat room sex offender: Has the internet enabled a new typology of sex offender? *Sexual Abuse, 23*(1), 72-91.

Broome, L. J., Izura, C., & Lorenzo-Dus, N. (2018). A systematic review of fantasy driven vs. contact driven internet-initiated sexual offences: Discrete or overlapping typologies? *Child Abuse and Neglect, 79*, 434-444.

Brophy, M. (2010). Sex, Lies, and Virtual Reality. In Allhoff, F., & Ponante, G. (Eds.). *Porn-Philosophy for Everyone: How to Think with Kink* (Vol. 30), pp204-218. London, UK: Wiley-Blackwell.

Brown, R., & Shelling, J. (2019). Exploring the implications of child sex dolls. *Trends and Issues in Crime and Criminal Justice, 570*, 1-13.

Carl, E., Stein, A. T., Levihn-Coon, A., Pogue, J. R., Rothbaum, B., Emmelkamp, P., Asmundson, G. J., Carlbring, P., & Powers, M. B. (2019). Virtual reality exposure therapy for anxiety and related disorders: A meta-analysis of randomized controlled trials. *Journal of Anxiety Disorders, 61*, 27–36. https://doi.org/10.1016/j.janxdis.2018.08.003

Castronova, E. (2008). *Synthetic worlds: The business and culture of online games*. University of Chicago press.

Cheung, M. (2012). *Child sexual abuse: Best practices for interviewing and treatment*. Chicago, USA: Lyceum Books.

Cornet, L. J., & Van Gelder, J. L. (2020). Virtual reality: A use case for criminal justice practice. *Psychology, Crime & Law*, 1-17.

Cripps, J., & Stermac, L. (2018). Cyber-Sexual Violence and Negative Emotional States among Women in a Canadian University. *International Journal of Cyber Criminology. 12*(1), 171-186.

Danaher, J. (2017a). Robotic rape and robotic child sexual abuse: should they be criminalised? *Criminal Law and Philosophy, 11*(1), 71-95.

Danaher J (2017b) Should we be thinking about robot sex? In: Danaher, J., & McArthur, N. (Eds.). (2017). *Robot sex: Social and ethical implications*. Cambridge, USA: MIT Press, pp.3-14.

Davidson, J., & Gottschalk, P. (2011). Characteristics of the internet for criminal child sexual abuse by online groomers. *Criminal Justice Studies, 24*(1), 23-36.

Davis, N., Lennings, C., & Green, T. (2018). Improving practice in child sexual abuse image investigations through identification of offender characteristics. *Sexual Abuse in Australia & New Zealand,* 1-12.

De Santisteban, P., Del Hoyo, J., Alcázar-Córcoles, M. Á., & Gámez-Guadix, M. (2018). Progression, maintenance, and feedback of online child sexual grooming: A qualitative analysis of online predators. *Child Abuse and Neglect, 80*, 203-215.

DeLong, R., Durkin, K., & Hundersmarck, S. (2010). An exploratory analysis of the cognitive distortions of a sample of men arrested in internet sex stings. *Journal of Sexual Aggression, 16*(1), 59-70.

DeMarco, J., Cheevers, C., Davidson, J., Bogaerts, S., Pace, U., Aiken, M., Caretti, V., Schimmenti, A., & Bifulco, A. (2017). Digital dangers and cyber-victimisation: A study of European adolescent online risky behaviour for sexual exploitation. *Clinical Neuropsychiatry, 14*(1), 104-112.

Demos (2018*). Technology briefing series: Briefing 1 online child sexual abuse imagery*. Retrieved on 10th March 2020 from https://www.demos.co.uk/wp-content/uploads/2018/01/Technology-Briefing-1-Online-CSAI-19.01-1.pdf

Devlin, K. (2018). *Turned On: Science, Sex and Robots*. London:Bloomsbury.

Doring, N. (2014). Consensual sexting among adolescents: Risk prevention through abstinence education or safer sexting? *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 8*(1), Article 9.

Durkin, K. F.. & Bryant, C. D. (1995). "Log on to sex": Some notes on the carnal computer and erotic cyberspace as an emerging research frontier,, *Deviant Behavior, 16*::3, 179-200, DOI: 10.1080/01639625.1995.9967998

Eggestein, J. V., & Knapp, K. J. (2014). Fighting Child Pornography: A Review of Legal and Technological Developments. *Journal of Digital Forensics, Security and Law, 9*(4), 29-48.

Eke, A. W., Seto, M. C., & Williams, J. (2011). Examining the criminal history and future offending of child pornography offenders: An extended prospective follow-up study. *Law and Human Behavior, 35*(6), 466-478.

El Asam, A., & Katz, A. (2018). Vulnerable young people and their experience of online risks. *Human–Computer Interaction, 33*(4), 281-304.

Elliott, I. A. (2017). A self-regulation model of sexual grooming. *Trauma, Violence, and Abuse, 18*(1), 83-97.

Elliott, I. A., Beech, A. R., Mandeville-Norden, R., & Hayes, E. (2009). Psychological profiles of internet sexual offenders: Comparisons with contact sexual offenders. *Sexual Abuse, 21*(1), 76-92.

Elliot, I.A., Mandeville-Norden, R., Rakestrow-Dickens, J., & Beech, A.R. (2019) Reofending rates in a UK community sample of individuals with convictions for indecent images of children. *Law and Human Behavior, 43*(4), 369-382.

Fortin, F., Paquette, S., & Dupont, B. (2018). From online to offline sexual offending: Episodes and obstacles. *Aggression and Violent Behavior*, 39, 33-41.

Fortin, F., & Proulx, J. (2019). Sexual interests of child sexual exploitation material (CSEM) consumers: Four patterns of severity over time. *International Journal of Offender Therapy and Comparative Criminology*, 63(1), 55-76.

Fromberger, P., Meyer, S., Kempf, C., Jordan, K., & Müller, J. L. (2015). Virtual viewing time: The relationship between presence and sexual interest in androphilic and gynephilic men. *PloS One*, 10(5), 1-35.

Galbraith, P. W. (2011). Lolicon: The reality of 'virtual child pornography' in Japan*. Image & Narrative, 12*(1), 83-119.

Garcia, B., Lopez, M. C., & Jimenez, A. (2014). The risks faced by adolescents on the internet: Minors as actors and victims of the dangers of the internet. *Revista Latina de Comunicación Social, 69*, 462-485.

Gaudiosi, J. (2016). Pornhub Adds Free Virtual Reality Section for Oculus, Google Cardboard. *Fortune*, March 23. [Online] Available: https://fortune.com/2016/03/23/pornhub-adds-free-virtual-reality-section-for-oculus-google-cardboard/ [Accessed 10 March 2020]

Ghani, N. (2016), *Now I know it was wrong: Report of the parliamentary inquiry into support and sanctions for children who display harmful sexual behaviour*, Barnardo's.

Gomes, M. L., & Wu, R. (2018). User evaluation of the neurodildo: A mind-controlled sex toy for people with disabilities and an exploration of its applications to sex robots. *Robotics*, *7*(3), 46-68.

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford, USA: Stanford University Press.

Hamilton-Giachritsis, C., Banakou, D., Quiroga, M. G., Giachritsis, C., & Slater, M. (2018). Reducing risk and improving maternal perspective-taking and empathy using virtual embodiment. *Scientific Reports*, *8*(1), 1-10.

Hempel, I. S., Buck, N. M. L., Van Vugt, E. S., & Van Marle, H. J. C. (2015). Interpreting child sexual abuse: Empathy and offense-supportive cognitions among child sex offenders. *Journal of Child Sexual Abuse, 24*(4), 354-368.

Helmus, L., Hanson, R. K., Babchishin, K. M., & Mann, R. E. (2013). Attitudes supportive of sexual offending predict recidivism: A meta-analysis. *Trauma, Violence, and Abuse, 14*(1), 34-53.

Henshaw, M., Ogloff, J. R., & Clough, J. A. (2017). Looking beyond the screen: A critical review of the literature on the online child pornography offender. *Sexual Abuse, 29*(5), 416-445.

Hirschtritt, M. E., Tucker, D., & Binder, R. L. (2019). Risk Assessment of Online Child Sexual Exploitation Offenders. *The Journal of the American Academy of Psychiatry and the Law, 47*(2), 155-164.

Houtepen, J. A., Sijtsema, J. J., & Bogaerts, S. (2014). From child pornography offending to child sexual abuse: A review of child pornography offender characteristics and risks for cross-over. *Aggression and Violent Behavior, 19*(5), 466-473.

Internet Watch Foundation. (2018). *Trends in online child sexual exploitation: Examining the distribution of captures of live-streamed child sexual abuse*. Available: https://www.iwf.org.uk/sites/default/files/inline-files/Distribution%20of%20Captures%20of%20Live-streamed%20Child%20Sexual%20Abuse%20FINAL.pdf [Accessed 10th March 2020]

Jonsson, L. S., Svedin, C. G., & Hydén, M. (2014). " Without the internet, I never would have sold sex": Young women selling sex online. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *8*(1), 1-14.

Kettleborough, D. G., & Merdian, H. L. (2017). Gateway to offending behaviour: permission-giving thoughts of online users of child sexual exploitation material. *Journal of Sexual Aggression, 23*(1), 19-32.

Klein, C. A. (2014). Digital and divergent: sexual behaviors on the internet. *Journal of the American Academy of Psychiatry and the Law, 42*(4), 495-503.

Kloess, J. A., Beech, A. R., & Harkins, L. (2014). Online child sexual exploitation: Prevalence, process, and offender characteristics. *Trauma, Violence, and Abuse, 15*(2), 126-139.

Kloess, J. A., Seymour-Smith, S., Hamilton-Giachritsis, C. E., Long, M. L., Shipley, D., & Beech, A. R. (2017). A qualitative analysis of offenders' modus operandi in sexually exploitative interactions with children online. *Sexual Abuse, 29*(6), 563-591.

Koops, T., Dekker, A., & Briken, P. (2018). Online sexual activity involving webcams—An overview of existing literature and implications for sexual boundary violations of children and adolescents. *Behavioral Sciences and the Law, 36*(2), 182-197.

Kopecký, K. (2017). Online blackmail of Czech children focused on so-called "sextortion" (analysis of culprit and victim behaviors). *Telematics and Informatics, 34*(1), 11-19.

Krasodomski-Jones, A. (2018). *Online Child Sexual Abuse Imagery (Tech Education Project Paper 1).* Demos. [Online]. Available: https://demosuk.wpengine.com/wp-content/uploads/2018/01/Technology-Briefing-1-Online-CSAI-19.01-1.pdf ([Accessed 30 March 2020)]

Levy, N. (2002). Virtual child pornography: The eroticization of inequality. *Ethics and Information Technology, 4*(4), 319-323.

Li, J. J., Ju, W., & Reeves, B. (2017). Touching a mechanical body: tactile contact with body parts of a humanoid robot is physiologically arousing. *Journal of Human-Robot Interaction, 6*(3), 118-130.

Livingstone, S., & Bober, M. (2005). *UK children go online: Final report of key project findings*. London, UK: LSE Research Online.

Livingstone, S., & Smith, P. K. (2014). Annual research review: Harms experienced by child users of online and mobile technologies: The nature, prevalence, and management of sexual and aggressive risks in the digital age. *Journal of Child Psychology and Psychiatry, 55*(6), 635-654.

Long, M. L., Alison, L. A., & McManus, M. A. (2013). Child pornography and likelihood of contact abuse: A comparison between contact child sexual offenders and noncontact offenders. *Sexual Abuse, 25*(4), 370-395.

Lorenzo-Dus, N., & Izura, C. (2017). "Cause ur special": Understanding trust and complimenting behaviour in online grooming discourse. *Journal of Pragmatics, 112*, 68-82.

Lowry, P. B., Zhang, J., Moody, G. D., Chatterjee, S., Wang, C., & Wu, T. (2019). An integrative theory addressing cyberharassment in the light of technology-based opportunism. *Journal of Management Information Systems, 36*(4), 1142-1178.

Lynch, M. J. (2010). Sex work in Second Life: Scripts, presence, and bounded authenticity in a virtual environment. *Social Thought and Research, 31*, 37-56.

Malesky Jr, L. A. (2007). Predatory online behavior: Modus operandi of convicted sex offenders in identifying potential victims and contacting minors over the internet. *Journal of Child Sexual Abuse, 16*(2), 23-32.

Malloy, K. M., & Milling, L. S. (2010). The effectiveness of virtual reality distraction for pain reduction: A systematic review. *Clinical Psychology Review*, *30*(8), 1011-1018.

Maras, M. H., & Shapiro, L. R. (2017). Child sex dolls and robots: More than just an uncanny valley. *Journal of Internet Law, 21,* 3-17.

Marcum, C. D. (2007). Interpreting the intentions of internet predators: An examination of online predatory behavior. *Journal of Child Sexual Abuse, 16*(4), 99-114.

Martellozzo, E. (2017). Online sexual grooming: Children as victims of online abuse. In *Cybercrime and Its Victims* (pp. 124-144). London, UK: Routledge.

Martin, J. (2014). "It's Just an Image, Right?" Practitioners' Understanding of Child Sexual Abuse Images Online and Effects on Victims. *Child and Youth Services, 35*(2), 96-115.

Martin, J. (2015). Conceptualizing the harms done to children made the subjects of sexual abuse images online. *Child and Youth Services, 36*(4), 267-287.

Matamala-Gomez, M., Donegan, T., Bottiroli, S., Sandrini, G., Sanchez-Vives, M. V., & Tassorelli, C. (2019). Immersive virtual reality and virtual embodiment for pain relief. *Frontiers in Human Neuroscience*, *13*, 279-301.

Mathur, M. B., & Reichling, D. B. (2016). Navigating a social world with robot partners: A quantitative cartography of the Uncanny Valley. *Cognition, 146*, 22-32.

Mitchell, D. (1995). From MUDs to virtual worlds. [Online] http://mentallandscape.com/Papers_95vworlds.htm (Accessed 30 March 2020)

Montiel, I., & Agustina, J. R. (2019). Educational challenges of emerging risks in cyberspace: Foundations of an appropriate strategy for preventing online child victimisation. *Spanish Pedagogy Magazine 77*(273), 277-294.

Mori, M. (2012). The uncanny valley. *IEEE Robotics & Automation Magazine, Issue 2* (June), 98 - 100.

Munro, K. (2002). Conflict in cyberspace: How to resolve conflict online. *The Psychology of Cyberspace*, *7*(3), 321-326.

Munster, G., Jakel, T., CLinton, D., & Murphy, E. (2015). *Next mega tech theme is virtual reality.* Minneapolis, MN: Piper Jaffray Investment Research.

Nair, A. (2010). Real porn and pseudo porn: The regulatory road. *International Review of Law, Computers and Technology, 24*(3), 223-232.

Narumi T., Nishizaka S., Kajinami T., Tanikawa T., & Hirose M. (2011) *Meta Cookie+: An Illusion-Based Gustatory Display*. In: Shumaker R. (eds) Virtual and Mixed Reality - New Trends. VMR 2011. Lecture Notes in Computer Science, vol 6773. Springer, Berlin, Heidelberg

National Crime Agency (2019). *National strategic assessment of serious and organised crime.* Available: https://issuu.com/nca_uk/docs/official_nsa_-

_final_for_web_8d54fba93a80de?embed_cta=read_more&embed_context=embed&embed_domain=nationalcrimeagency.gov.uk (Accessed 28 March 2020)

Neutze, J., Seto, M. C., Schaefer, G. A., Mundt, I. A., & Beier, K. M. (2011). Predictors of child pornography offenses and child sexual abuse in a community sample of pedophiles and hebephiles. *Sexual Abuse, 23*(2), 212-242.

Ost, S. (2016). A new paradigm of reparation for victims of child pornography. *Legal Studies, 36*(4), 613-638.

Ost, S., & Gillespie, A. A. (2019). To know or not to know: should crimes regarding photographs of their child sexual abuse be disclosed to now-adult, unknowing victims? *International Review of Victimology*, *25*(2), 223-247.

Owens, E. W., Behun, R. J., Manning, J. C., & Reid, R. C. (2012). The impact of internet pornography on adolescents: A review of the research. *Sexual Addiction and Compulsivity, 19*(1-2), 99-122.

Owens, J. N., Eakin, J. D., Hoffer, T., Muirhead, Y., & Shelton, J. L. E. (2016). Investigative aspects of crossover offending from a sample of FBI online child sexual exploitation cases. *Aggression and Violent Behavior, 30*, 3-14.

Palmer, T. (2015). *Digital dangers: The impact of technology on the sexual abuse and exploitation of children and young people.* London, UK: Barnados

Paquette, S., & Cortoni, F. (2020). Offense-supportive cognitions expressed by men who use internet to sexually exploit children: A thematic analysis. *International Journal of Offender Therapy and Comparative Criminology,* 66:6-7, pp 647-669

Paquette, S., Longpre, N., & Cortoni, F. (2020). A billion distorted thoughts: An exploratory study of criminogenic cognitions among men who sexually exploit children over the Internet. *International journal of offender therapy and comparative criminology*, 64(10-11), 1114-1133.

Peck, T. C., Seinfeld, S., Aglioti, S. M., & Slater, M. (2013). Putting yourself in the skin of a black avatar reduces implicit racial bias. *Consciousness and Cognition*, *22*(3), 779-787.

Pezzutto, S. (2019). From porn performer to porntropreneur: Online entrepreneurship, social media branding, and selfhood in contemporary trans pornography. *AG About Gender-Rivista internazionale di studi di genere*, *8*(16), 30-60.

Quayle, E., & Cooper, K. (2015). The role of child sexual abuse images in coercive and non-coercive relationships with adolescents: A thematic review of the literature. *Child and Youth Services, 36*(4), 312-328.

Quayle, E., & Taylor, M. (2001). Child seduction and self-representation on the internet. *CyberPsychology and Behavior, 4*, 597–608.

Quayle, E., & Taylor, M. (2002). Child pornography and the internet: Perpetuating a cycle of abuse. *Deviant Behavior, 23*(4), 331-361.

Quayle, E., & Taylor, M. (2003). Model of problematic internet use in people with a sexual interest in children. *Cyberpsychology and Behavior*, *6*(1), 93-106.

Ramiro, L. S., Martinez, A. B., Tan, J. R., Mariano, K., Miranda, G. M., & Bautista, G. (2019). Online child sexual exploitation and abuse: A community diagnosis using the social norms theory. *Child Abuse and Neglect*, 1-15.

Reeves, C. (2012). Blurring Fantasy and Action: the problem of virtual sexual ageplay. In: *British Society of Criminology Conference 2012: 'Criminology at the Borders'*, Portsmouth, UK. (Unpublished)

Reeves, C. (2013). Fantasy depictions of child sexual abuse: The problem of ageplay in Second Life. *Journal of Sexual Aggression, 19*(2), 236-246.

Reeves, C. (2018). The virtual simulation of child sexual abuse: online gameworld users' views, understanding and responses to sexual ageplay. *Ethics and Information Technology, 20*(2), 101-113.

Riegel, D. L. (2004). Effects on boy-attracted pedosexual males of viewing boy erotica (letter to the editor). *Archives of Sexual Behaviour, 33,* 321-323.

Renaud, P., Trottier, D., Rouleau, J. L., Goyette, M., Saumur, C., Boukhalfi, T., & Bouchard, S. (2014). Using immersive virtual reality and anatomically correct computer-generated characters in the forensic assessment of deviant sexual preferences. *Virtual Reality, 18*(1), 37-47.

Renaud, P., Trottier, D., Rouleau, J. L., Goyette, M., Saumur, C., Boukhalfi, T., & Bouchard, S. (2014). Using immersive virtual reality and anatomically correct computer-generated characters in the forensic assessment of deviant sexual preferences. *Virtual Reality, 18*(1), 37-47.

Renaud, P., Nolet, K., Chartier, S., Trottier, D., Goyette, M., Rouleau, J. L., Proulx, J., & Bouchard, S. (2012). Sexual presence and intentional dynamics: Deviant and non-deviant sexual self-regulation from the first-person stance. *Journal of Eye Tracking, Visual Cognition and Emotions, 2*(1), 82-96.

Reyns, B. W., Burek, M. W., Henson, B., & Fisher, B. S. (2013). The unintended consequences of digital technology: Exploring the relationship between sexting and cybervictimization. *Journal of Crime and Justice, 36*(1), 1-17.

Rimer, J. R. (2017). Internet sexual offending from an anthropological perspective: Analysing offender perceptions of online spaces. *Journal of Sexual Aggression, 23*(1), 33-45.

Rimer, J. R. (2019). "In the street they're real, in a picture they're not": Constructions of children and childhood among users of online child sexual exploitation material. *Child Abuse and Neglect, 90,* 160-173.

Russell, G. (2007). Pedophiles in wonderland: Censoring the sinful in cyberspace. *Journal of Criminal Law and Criminology, 98,* 1467-1500.

Saramago, M. A., Cardoso, J., & Leal, I. (2019). Pornography use by sex offenders at the time of the index offense: Characterization and predictors. *Journal of Sex and Marital Therapy, 45*(6), 473-487.

Say, G. N., Babadağı, Z., Karabekiroğlu, K., Yüce, M., & Akbaş, S. (2015). Abuse characteristics and psychiatric consequences associated with online sexual abuse. *Cyberpsychology, Behavior, and Social Networking, 18*(6), 333-336.

Schulz, A., Bergen, E., Schuhmann, P., Hoyer, J., & Santtila, P. (2016). Online sexual solicitation of minors: How often and between whom does it occur? *Journal of Research in Crime and Delinquency, 53*(2), 165-188.

Seinfeld, S., Arroyo-Palacios, J., Iruretagoyena, G., Hortensius, R., Zapata, L. E., Borland, D., de Gelder, S., & Sanchez-Vives, M. V. (2018). Offenders become the victim in virtual reality: Impact of changing perspective in domestic violence. *Scientific Reports*, *8*(1), 1-11.

Seto, M. C., & Eke, A. W. (2005). The criminal histories and later offending of child pornography offenders. *Sexual Abuse: A Journal of Research and Treatment, 17*(2), 201-210.

Seto, M. C., & Eke, A. W. (2015). Predicting recidivism among adult male child pornography offenders: Development of the Child Pornography Offender Risk Tool (CPORT). *Law and Human Behavior, 39*(4), 416.

Seto, M. C., Hanson, K. R., & Babchishin, K. M. (2011). Contact sexual offending by men with online sexual offenses. *Sexual Abuse, 23*(1), 124-145.

Shannon, D. (2008). Online sexual grooming in Sweden—Online and offline sex offences against children as described in Swedish police data. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, *9*(2), 160-180.

Shaw, D. (2017). The 'new phenomenon' of child sex dolls. BBC News. Available: https://www.bbc.co.uk/news/uk-40776621 [Accessed 14 January 2020.]

Sheehan, V., & Sullivan, J. (2010). A qualitative analysis of child sex offenders involved in the manufacture of indecent images of children. *Journal of Sexual Aggression, 16*(2), 143-167.

Shriram, K., & Schwartz, R. (2017). All are welcome: Using VR ethnography to explore harassment behavior in immersive social virtual reality. *IEEE Virtual Reality,* 225-226.

Simon, L. E., Daneback, K., & Ševčíková, A. (2014). The educational dimension of pornography: Adolescents' use of new media for sexual purposes. *Living in the Digital Age,* 33-48.

Sklenarova, H., Schulz, A., Schuhmann, P., Osterheider, M., & Neutze, J. (2018). Online sexual solicitation by adults and peers–Results from a population based German sample. *Child Abuse and Neglect, 76*, 225-236.

Slater, M., & Sanchez-Vives, M. V. (2016). Enhancing our lives with immersive virtual reality. *Frontiers in Robotics and Artifical Intelligence*, *3*, 1-47.

Snodgrass, J. G., Lacy, M. G., Dengah, H. F., Fagan, J., & Most, D. E. (2011). Magical flight and monstrous stress: Technologies of absorption and mental wellness in Azeroth. *Culture, Medicine, and Psychiatry*, *35*(1), 26-62.

Soldino, V., Carbonell-Vayá, E. J., & Seigfried-Spellar, K. C. (2019). Criminological differences between child pornography offenders arrested in Spain. *Child Abuse and Neglect, 98,* 1-18.

Sparrow, R. (2017). Robots, rape, and representation. *International Journal of Social Robotics*, 9(4), 465-477.

Steel, C. M., Newman, E., O'Rourke, S., & Quayle, E. (2020). An integrative review of historical technology and countermeasure usage trends in online child sexual exploitation material offenders. *Forensic Science International: Digital Investigation, 33*, 300971.

Stuart, R. (2017). Webcamming: the sex work revolution that no one is willing to talk about. [Online] https://theconversation.com/webcamming-the-sex-work-revolution-that-no-one-is-willing-to-talk-about-69834 (Accessed 30 March 2020)

Su, N. M., Lazar, A., Bardzell, J., & Bardzell, S. (2019). Of dolls and men: Anticipating sexual intimacy with robots. *ACM Transactions on Computer-Human Interaction (TOCHI), 26*(3), 1-35.

Suler, J. (2004). The online disinhibition effect. *Cyberpsychology and Behavior, 7*(3), 321-326.

Suler, J. R. (2016). *Psychology of the digital age: Humans become electric*. Cambridge University Press.

Svedin, C. G., & Priebe, G. (2009). Youth, sex, and the internet. In *Youth Board, 9*, 32-143.

Taylor, M. (2000). The nature and dimensions of child pornography on the internet', paper prepared for the *International Conference' Combating Child Pornography on the Internet*', Vienna, Austria, 29 September to 1 October 1999.

Thorn (2020). *Self-Generated Child Sexual Abuse Material: Attitudes and Experiences Complete findings from 2019 qualitative and quantitative research among 9–17-year-olds and caregivers*. Available: https://info.thorn.org/hubfs/Research/08112020_SG-CSAM_AttitudesExperiences-Report_2019.pdf [Accessed 23 May 2022]

Ticknor, B. (2019). Virtual reality and correctional rehabilitation: A game changer. *Criminal Justice and Behavior, 46*(9), 1319-1336.

Triberti, S., Repetto, C., & Riva, G. (2014). Psychological factors influencing the effectiveness of virtual reality–based analgesia: A systematic review. *Cyberpsychology, Behavior, and Social Networking*, *17*(6), 335-345.

Turley, C. (2012). *European Online Grooming Project*. NatCen Social Research.

US National Centre for Missing and Exploited Children (NCMEC). (2018). *The issues: Online enticement.* Available: https://www.missingkids.org/theissues/onlineenticement [Accessed 20 April 2020]

Wang, S., Lilienfeld, S. O., & Rochat, P. (2015). The uncanny valley: Existence and explanations. *Review of General Psychology, 19*(4), 393-407.

Ward, T., & Keenan, T. (1999). Child molesters' implicit theories. *Journal of Interpersonal Violence, 14*(8), 821-838.

Weeden, S., Cooke, B., & McVey, M. (2013). Underage children and social networking. *Journal of Research on Technology in Education, 45*(3), 249-262.

Wiederhold, B. K. & Bouchard, S., (2014) *Advances in virtual reality and anxiety disorders*. 2014. https://doi.org/10.1007/978-1-4899-8023-6

Wilson, R. (2009). Sex play in virtual worlds. *Washington and Lee Law Review, 66*(3), 1127-1174.

Winters, G. M., Kaylor, L. E., & Jeglic, E. L. (2017). Sexual offenders contacting children online: An examination of transcripts of sexual grooming. *Journal of Sexual Aggression, 23*(1), 62-76.

Whittle, H. C., Hamilton-Giachritsis, C. E., & Beech, A. R. (2014). "Under his spell": Victims' perspectives of being groomed online. *Social Sciences, 3*(3), 404-426.

Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Collings, G. (2013). A review of online grooming: Characteristics and concerns. *Aggression and Violent Behavior, 18*(1), 62-70.

Wolak, J., Finkelhor, D., Mitchell, K. J., & Ybarra, M. L. (2010). Online "predators" and their victims: Myths, realities, and implications for prevention and treatment. *American Psychologist, 63*(2), 111-128.

Wright, P., Tokunaga, R.S., & Kraus, A. (2016) A meta-analysis of pornography consumption and actual acts of sexual aggression in general population studies. Journal of Communication, 66, 183-205.

Appendix 1: Definitions

Summary of relevant definitions used by the National Crime Agency's Child Exploitation and Online Protection team, see https://www.ceop.police.uk/Safety-Centre/what-is-online-child-sexual-abuse/

Online grooming	The act of developing a relationship with a child to enable their abuse and exploitation both online and offline. Online platforms, such as social media, messaging and live streaming apps, can be used to facilitate this offending.
Live streaming	Live streaming services can be used by offenders to incite victims to commit or watch sexual acts via webcam. Offenders also stream or watch live contact sexual abuse or indecent images of children with other offenders. In some instances, offenders will pay facilitators to stream live contact abuse, with the offender directing what sexual acts are perpetrated against the victim.
Online coercion and blackmail	The coercion or blackmail of a child by technological means, using sexual images and/or videos depicting that child, for the purposes of sexual gain (e.g., to obtain new indecent images of children or bring about a sexual encounter), financial gain or other personal gain.
Indecent Images of Children (IIOC)	Indecent Images of Children (IIOC) are images of, or depicting, a child or part of a child, which are judged to be in breach of recognised standards of propriety. Examples of images considered to be indecent are those depicting a child engaging in sexual activity or in a sexual manner, through posing, actions, clothing etc. IIOC includes photographs, videos, pseudo-photographs, and tracings.
Prohibited images of children	Prohibited images of children are non-photographic images, for example CGI, cartoons etc, which portray a child engaging in sexual activity, a sexual act being performed in the presence of a child or focus on the child's genital or anal region.
Possession, production and sharing of images	Child sexual offenders can use online platforms to store and share Indecent Images of Children (IIOC) and prohibited images. Online platforms can also be used to facilitate the production of IIOC, for example screen-recording of CSEA perpetrated over live streaming.

Appendix 2: Methodology

We were funded for a three-month project to provide an initial overview of research and 'grey literature' on the use of Extended Reality (XR) technologies in online child sexual exploitation and abuse, including on the likely scale and spread of XR and related technologies, and the potential impact (on victims and abusers) of this type of OCSEA. Our scope included virtual reality, mixed reality, augmented reality, and associated technology (e.g., teledildonics, dolls).

Evidence reviews and synthesis

At the start of the project, we held discussions with funders about the scope and scale of the project and we shared initial thoughts on direction of the research.

The team first worked separately on evidence syntheses. KH led a rapid review of research and other literature on online child sexual exploitation (sections 1 and 3), with oversight and support from PT, SF and EB. Four electronic databases; Scopus, Web of Science, ProQuest, and Criminal Justice Abstracts were searched using the following terms, using Boolean operators, truncations, and alternative spellings: virtual reality, augmented reality, mixed reality, simulation, immersive technology, telepresence, cyberspace, abuse, exploitation, harassment, sexual exploitation, sexual abuse, sexual harassment, grooming, pornography, cybercrime, child, minor. The search string was altered as necessary for each database, and reference lists, relevant journals and grey literature were hand-searched to identify papers not captured through electronic searches.

Titles and abstracts were assessed for relevance and of those deemed relevant full papers were assessed to determine inclusion. Articles were included if OCSEA or technology-facilitated abuse were the primary focus. Duplicates were identified and removed. No date restrictions were applied. Only papers published in English were considered. A total of 6937 papers were identified in the search. The titles and abstracts of 349 papers, and the full texts of 240 papers were assessed. Approximately 150 eligible papers were used to inform the report. In addition, EB conducted a light (non-systematic) review of literature on adult online sex work.

SP/JM built a taxonomy of key concepts in XR and led a rapid review of the current scope and state of the art, drawing on recent journal, conference, and general technology media publications in the area. This was then expanded to create the overview of XR technology (section 2).

After completing the draft evidence reviews and literature synthesis, team members met on several occasions to integrate the findings from social/behavioural science and computer science (sections 3 and 4).

In early 2022, we carried out a light pre-publication update of section 4, in light of a spate of recent developments relating to Facebook's rebranding as Meta and their foregrounding of the 'Metaverse' and acknowledging increasing anecdotal reports of harassment and 'grooming' behaviour in VR social spaces.

Limitations of the research

- Given the tight timescale and limited resources, we did not conduct full systematic reviews.
- We did not include literature from disciplines such as law and philosophy.
- We only included literature in the English language, introducing a publication bias. Research from other nations that are at the forefront of technological development in this area (e.g., Japan, Korea) that are not in the English language may have provided further insights.
- A systematic quality appraisal of the literature was not undertaken.

The impact of Covid-19

The report was completed in May 2020. It is likely that the Covid-19 pandemic will have had some impact on the development and uptake of XR technologies, their spread and use, and, potentially, the risk to children. A detailed review of such developments is outside the scope of this report, and it is still too early for robust evidence (as opposed to anecdotal evidence) on the impact of repeated global lockdowns.