Online sharenting: Identifying existing vulnerabilities and demystifying media reported crime risks

Online sharenting: identifying existing vulnerabilities and demystifying media reported crime risks

Abstract

Sharenting – the digital sharing of sensitive information of minors by parents or guardians – has not yet been investigated from a criminological perspective. However, there are reported concerns regarding its criminogenic potential amidst fast-growing media interest in sharenting practices, particularly in relation to the perceived crime risks. This article offers an exploratory analysis of cases where such practices led to the victimisation of minors, evidencing the gap between media reports about crime risks and actual victimisation. The paper also demonstrates that sharenting is a more complex phenomenon than generally recognised. By exploring these issues, the paper advances criminological understanding of the practice and demonstrates the divergences between media-reported crime risks and victimisation associated with sharenting. Although the paper highlights media exaggerations of such crime victimisation which can heighten public fear and anxiety, the article also provides new insights on the nature of actual victimisation, to raise awareness and aid preventative intervention.

Keywords

Sharenting; digital harms; digitised identity; risk; victimisation; crime vulnerabilities

Introduction

Especially over the past 15 years, the creation of new 'online identities' (the social identity that we acquire in cyberspace) and the expansion of the usability of our 'digital identity' (the digital storage of our attributed, biographical or even biological identities) have entailed, alongside many advantages, new and emerging crime risks as well as crime vulnerabilities[1]. A reason for this is that identity information can be misused in many ways, heightening the risks of identity theft and other crimes. Existing research in this context has so far focused on illegal access to personal information, for example through hacking or social engineering techniques, and can involve the manipulation of stored user data by social media companies to control attitudes and behaviours. Yet, the extant criminological literature has overlooked the risky behaviours of individuals willingly sharing identifying and potentially sensitive information online. In this context, an area of particular interest that has been relatively neglected is the one connected to so called sharenting practices – that is, the digital sharing of sensitive information of minors, who are often overexposed online in good faith by parents or guardians (hereafter, the 'sharenters'), or – to borrow Brosch's definition – the 'making public by parents a lot of detailed information about their children in the form of photos, videos and posts through social media, which violate children's privacy' (Brosch 2018: 78). Sharenting is not a niche behaviour: according to OFCOM (2017), almost half of UK parents sharing photos of their children online, making sharenting a 'modern dilemma'.

Sharenting, to the authors' knowledge, has not been investigated from a criminological perspective (with the recent exception of Lavorgna et al. 2022, originating from the same ESRC-project *ProTechThem: Building Awareness for Safer and Technology-Savvy*

[1] Crime risks are here broadly conceptualized as ascertainable dangers, whose probability to occur can be minimized through rational decisions (e.g., Hollway and Jefferson 19979. Crime vulnerabilities are here broadly conceptualized as structural, systemic dangers (see, e.g., Walklate 2011; Brown et al. 2017).

Sharenting[2]). Existing publications on this topic mainly stem from law (Steinberg 2017; Hancock 2021), media, communication and cultural studies (Choi and Lewallen 2018; Ouvrein and Verswijvel 2019; Siibak and Traks 2019; Verswijvel et al. 2019; Blum-Ross and Livingstone 2017; Barnes and Potter 2021; Jorge et al. 2021); computer science (Ammari et al. 2015); educational sciences (Brosch 2018); and psychology (Lazard et al. 2019; Briazu et al. 2021). Additionally, there have been some journalistic inquiries on the topic (e.g., Coughlan 2018; Saner 2018; Bonanomi 2020). This growing scholarship and media interest reflects and heightens the curiosity and attention that the general public has on an increasingly common social practice.

Beyond the psychological or social risks posed by negative repercussions in ignoring children's desire to having (or not) an online identity (Steinberg 2017) or due to the perpetuation of gender and racial stereotypes (Choi and Lewallen 2018), there are concerns regarding the potential for grooming and child abuse, cyber hate, and identity crimes (e.g., Minkus et al. 2015; Bezáková et al. 2021; Wachs et al. 2021; Williams-Ceci et al. 2021). Through sharenting, it can be possible to identify a child's home, school or play location, be knowledgeable about a child physical or mental health issues, know about other potential vulnerabilities. As such, sharenting practices and their risks in terms of criminogenic features and social harms warrant attention also from a criminological perspective. A preliminary puzzle that needs to be solved, however, is whether and how sharenting practices are in fact enabling or facilitating crimes or other non-criminalized yet harmful activities. Consider, for instance, certain forms of digital harassment against minors. In existing studies and publications on the topic, potential crime and harm risks are assumed, with no substantiating data or other relevant evidence. This is in part because media reports about the practice emphasise *potential* risks (as detailed in the following section) although the extent and contexts of actual victimisation (where a harm, criminalised or not, is suffered) is not known.

The aim of this exploratory contribution is to offer some answers to this puzzle by analysing open-source media to determine specific media reports about the sharenting practices that have led to actual victimisation of minors. The paper also aims to assess media reports about the *risks* of crime and harms associated with sharenting – reports that are capable of influencing perceptions about such risks. To these ends the media analysis will focus on (i) the role of online platforms (e.g., systemic vulnerabilities and criminogenic effects), (ii) who the sharenters are and their reported motivation, (iii) crimes and offenders associated with sharenting practices, (iv) types of information shared, (v) responses and reactions to crime/harm risks and actual victimisation linked to sharenting, and (vi) specific points of vulnerability in sharenting processes (highlighted through the creation of a master script).

Our primary motivation for conducting this study is twofold. One relates to the importance of understanding whether and how media reported risks and crime victimisation could be fuelling assumptions about crime risks. We are also motivated by the need to understand contextual factors where such victimisation does occur, in order to raise awareness and address the gap in the criminological literature. The gap is indeed surprising given the growing realisation that, as we advance through the digital age, it has become increasingly important to protect digitised identity information from misuse, which is associated with serious physical, psychological/emotional and financial harms (Agrafiotis et al. 2018; Burnes et al. 2020; Lavorgna 2020). Sharenting is a practice that could impede children's ability to protect their

[2] http://www.protechthem.org/.

identity as they grow and become adults. Below we explore the importance of protecting one's digitised identity, in more detail.

Protecting digitised identity information: prospects, impediments, and media exaggerations

'Identity' is a multidimensional concept, which relates to notions of self-image, individuality, and social presentation; in other words, our persona, how we present ourselves to the world. Legal concepts of identity aim to distinguish one person from another, for instance by using the 'attributed identity' we acquire at birth (such as our name and date of birth), the 'biographical identity' we acquire during our lives (including qualifications and passports), or the 'biometric identity' that depends on certain physical characteristics (for example, fingerprints and iris patterns) (Clough 2015). Furthermore, in cyberspace we also acquire an 'online identity' – that is, a new social identity (or more identities) which may, or may not coincide with our real name (Papaioannou et al. 2019).

An expansion of the usability of our digital (or, to be more precise, digitally stored) identity is occurring in many Western countries, including the United Kingdom: the idea is to develop a common approach to digital identity for public services by making use of some attributes of an identity. Examples include name, address, date of birth and possibly biometrics which are used for different services as appropriate, in order to make digital identity services available to all individuals in a safer, secure, effective, proportionate, easy to use, accessible and cost-effective way (Feher 2021). Also, the private sector has been investing in the development of trusted digital identity and related data management systems (Taaffe 2019). Despite the many advantages, digitised identity information – as discussed in the following section – can be misused, leaving those involved in sharenting practices grappling with profound ethical dilemmas, as risks are introduced towards the same minors that should be safeguarded by the sharenters (Blum-Ross and Livingstone 2017).

So far, criminological research has focused on how human-based or technology-based social engineering[3] facilitates crimes enabled or facilitated by the misuse of digitised identity information (such as in phishing practices, see Holt and Turner 2012; Williams 2016; Lavorgna 2020; Steinmetz 2021). In neighbouring or interdisciplinary fields such as cybersecurity studies, there has been a surge in the use of biometric tools (such as thumbprint recognition in many smartphones) to counter such manipulative mechanisms and prevent identity misuse (Kolaczek 2009; Moskovitch et al. 2009). Manipulative mechanisms in this context refer to the increasingly advanced technologies and deceptive devices that perpetrators of cybercrime use to elicit sensitive information from unsuspecting victims and perpetrate identity crimes. The criminological and cybersecurity research on cybercrime provides useful insights into the nature of such devices (Bossler and Berenblum 2019; Lavorgna 2020). Examples include the high-definition cameras perpetrators use to capture data from images posted online, such as fingerprints (Muncaster 2019), and the hacking software they use to illegally access victims' electronic devices and steal data for various forms of identity misuse (Brey 2017).

Insights from the criminological literature on cybercrime highlight the harmful outcomes of identity misuse. For example, in Button and colleagues' (2021) study of how the victims of various forms of computer misuse perceive and experience the crime, the victims interviewed

[3] That is, skilfully manipulating an individual to take action in some aspects of their life.

described the impact as comparable, and, in some cases, more serious than physical crimes such as burglary. Victims described serious psychological harms including emotional distress caused by the digital intrusion and the feeling that they been violated even in cases where no financial loss had been incurred. In this context, computer misuse can involve cyber-dependent crimes such as the use of software and other digital technologies to illegally obtain data posted by sharenters.

Interestingly, however, researchers have long overlooked those cases in which individuals willingly share potentially sensitive information online, without any social engineering taking place, with only very recent research exploring ways to intervene and alter, for instance, parents' attitudes toward posting about their children online (Williams-Ceci et al. 2021). Think, for instance, of the wealth of information (including photos) shared on social media on a daily basis out of the desire to keep friends and relatives updated on life events, to grow and nourish social relationships, or more generally because 'sharing' increases some people's well-being (Berger and Buechel 2012).

In terms of the voluntary dissemination of sensitive information online, an area of particular interest that has been ignored in criminological discourse is the one connected to the sharing of potentially sensitive information of minors, or sharenting. On the one hand, minors might not be considered old enough to use their personal data to open, for instance, a bank account or even to enrol in some social media. On the other hand, some are being overexposed online, at times even before they are born, with parents sharing their private and often potentially sensitive information on social and digital media (Nottingham 2019), enabled by the architectural features of social media platforms that can trigger or exacerbate sharenting risks and harms (as discussed in detail by Lavorgna et al. 2022). There is an important tension between the desire to share online and the risk of misuse of the potentially sensitive identity information shared (see also Lavorgna et al. 2022). Consider, for instance, how posts on social media (and the pictures or videos often accompanying them), especially on parenting, travel or health-related groups, can include details of where you live/are, date of birth (e.g., a birthday photo), and health-related information among other things. Including minors in posts about political issues could also vicariously ascribe a political identity to affected minors long before they are old enough to establish one of their own. It is important to note that in most countries there are currently no policies securing children's right to online privacy, and the decision on whether and how to disclose information online is left to the parents or guardians (Lavorgna et al. 2022). This makes them the 'digital custodians' (Buchanan et al. 2019: 175) of the personal information of their children online, but they are often unprepared to the role (Steinberg 2017; Brosch 2018).

Furthermore, technological innovations can increase the unintended sharing of even biometric information: researchers in biometric security have warned that with the technological improvements in camera resolution professional criminals can 'steal' fingerprints details (which are very sensitive biometric data) from certain pictures (Muncaster 2019). Some of these data could expose minors to unwanted attention, both in the short-term (e.g., they might be targeted by ill-intentioned persons) and in the middle or even long-term periods. Indeed, today's children, in a few years, will be those employing digital identities in many aspects of their lives – ranging from education and health to business and democratic citizenship. They will need a clean and curated digital identity to be fully part of many aspects of our society, but the hygiene of their digital identities might be hard to obtain as certain sharenting practices mean that the wealth of information available about them could be exploited. In the current digital era of big data availability and accompanying datafication, the use of social media data

(in this case, images) to profile children is another sharenting risk that warrants attention (Saner 2018).

It is also important to protect digitised identity information not least because identity-related crimes are becoming increasingly connected to cyberspace. Identity crimes can take two main forms: identity theft and identity fraud [4]. A study by Barclays bank forecasted that sharenting will account for two thirds of identity fraud affecting young people by 2030 (as reported in *BBC* 2018). In addition, identity information can be misused to enable other serious crimes including grooming and various forms of abuse, as it allows the offender to obtain important data to better target their victims (Kloess et al. 2019; Lavorgna 2020; Bezáková et al. 2021; Wachs et al. 2021; Williams-Ceci et al. 2021). And of course, as anticipated above, beyond criminalised activities there are a number of non-criminalised yet harmful behaviours that can exploit identity-related information to harass victims even if they do not meet the legal threshold[5]. Overall, the misuse of identity information can produce adverse implications. In addition to direct physical, financial, social and emotional harms (see among others Steinberg 2017; Archer 2019; Barassi 2019; Lazard et al. 2019), victims could expend considerable time and effort restoring their credit, name, and reputation as the grow older. Furthermore, this issue can seriously undermine a victim's sense of trust, even of self (Golladay and Holtfreter 2017), and undermine digital inclusion (Monahan 2009; Roberts et al. 2012; Department for Digital, Culture, Media & Sport 2020a).

With the advent of data-driven technological advances now transforming the landscape of social interaction, digital inclusion has become a vital aspect of social life and policy making, and has been directly linked to broader processes of social inclusion (Sanders 2020). One of the official definitions of digital inclusion focuses on 'having the right access, skills, motivation and trust to confidently go online' (Department for Digital, Culture, Media & Sport 2020b). This suggests that everyone should be able to benefit from informational, interactional, and other resources associated with accessing online spaces without risks of identity-related crimes and other harms. Such access to online resources is a dimension of digital inclusion that is vital for social participation. It can determine whose voice is heard when online data are analysed to inform policy making, service delivery, and other key outcomes. But the risks of digital crimes and harms can discourage online participation and hence impede digital inclusion.

Only a few, very recent studies are starting to stress some of the risks related to exposing minors' lives online, often without their knowledge or informed consent. The focus has been on how children's desires in building (or not) an online identity are ignored (Nottingham 2019) or on the psychological repercussion of overexposure (Orlando 2017). Crime risks related to grooming and child abuse have been mentioned (by Minkus et al. 2015; Geddes 2019; Siibak 2019; Bezáková et al. 2021; Wachs et al. 2021; and Williams-Ceci et al. 2021 among others).

Put together, these and other often-cited risks of sharenting (Potter and Barnes 2021) could in part be informed by media reports about the practice and exaggerated crime risks. In criminological theory, media amplification or exaggeration of certain activities as risky can precipitate unnecessary fears and anxieties, which can in turn, provoke calls for punitive policy

[4] Identity theft occurs when the offender uses the personal information they obtained to impersonate one or more victims across a period of time spanning hours to years. Identity fraud can range from benefit and loan frauds to credit card and bank frauds (see Lavorgna 2020).

[5] On the importance to adopt a social harm approach in investigating the digital realm, and for the role of criminology in dealing with sociotechnical challenges, see Lavorgna 2021a,b.

intervention (Jewkes 2015). At the same time, it can distract from other forms of (less-newsworthy) victimisation, which might end up being overlooked.

Despite the increase in cybercrime and digital harms research in recent years, there is still a knowledge gap on whether the crime risks associated with sharenting often highlighted by the media are actually substantiated by the occurrence of actual crimes or other harmful activities committed against affected minors. Specifically, there is insufficient insight into the existence of specific cases where sharenting led to the victimisation of minors. There is also limited information on accompanying contextual information that can help raise evidence-based awareness. In the next section, we present our study which examined these issues by analysing real life cases reported in the media. This involved (1) identifying media reports discussing sharenting and its risks, (2) analysing the subset of these reports reporting specific cases where sharenting led to actual victimisation, and (3) exploring the contexts of the actual victimisation to raise awareness and possibly aid policy intervention.

Methodology

To identify relevant cases of sharenting leading to minors' victimisation, the researchers relied on the content aggregator Nexis to collect newspapers, magazines and journals, blogs, or other types of web-based publications published in English over the last ten years (1.1.2011 to 31.12.2021). The following syntax (as refined by the researchers after tentative keyword searches to minimise false negatives) was applied: '(minor OR child!) AND (parent OR mother OR father OR grandparent OR grandmother OR uncle OR aunt OR teacher) AND ((sharenting OR oversharing) OR (exposure near/5 information)) AND (crim! OR harm! OR danger!)'. The initial search yielded 1,379 results. These were manually screened for relevance, as we were only interested in publications offering information or references to cases where sharenting led to the victimisation of minors; despite the limited generalisability of this sampling method, it allowed for the inclusion of data with particular characteristics of interest. This strategy resulted in a final sample of 32 articles describing a total of 57 unique cases – a number that was significantly less than our expectations given the importance of the topic. This is nonetheless interesting as it signals that, despite the existence of many digital publications amplifying the crime risks of sharenting by associating the practice with various forms of victimisation, only few of them actually report real-life victimisation cases. The overwhelming majority refer solely to risks. Without substantiating evidence, such reports are capable of fuelling public fear and anxieties. Indeed, our initial finding regarding the paucity of relevant articles on the topic demonstrates that careful analysis of widely discussed social issues capable of triggering such public reaction is important to extract relevant evidence. This is the task the current study undertook.

The researchers carried out manual content analysis, categorising relevant passages in the text according to a coding framework agreed by all the researchers and summarised in Appendix A. The aim was to identify relevant codes and organise them for descriptive presentation of results. The process involved an abductive process of generating coherent patterns from the data; given the study's focus on sharenting, codes were categorised based on insights from emerging data and the scant sharenting literature.

Additionally, relevant information reported on the commission of the crimes or the otherwise harmful activities identified was organised through a crime script approach (a way to map the sequence of actions committed by offenders to deconstruct the crime-commission process) to

identify points of vulnerability to victimisation. Cornish (1994) elaborated the concept of 'crime scripts' to describe the essential stages of a criminal activity, making the decision points explicit in behavioural routines[6]. Crime scripts have been applied extensively over the past twenty years (e.g., Tremblay et al. 2001; Chiu et al. 2011; Leclerc et al. 2011; Lavorgna 2014, 2015; Leclerc 2017; Dehghanniri and Borrion 2021), mostly to identify the criminogenic opportunities exploited in criminal events with the aim to ideate situational crime prevention measures (Clarke 2008). However, script analysis is by definition crime-specific (Moreto and Clarke 2013), meaning that we had to adapt it (by broadening the level of analysis to the macro-level) to serve as a useful tool to organise harmful sharenting cases for analytical needs, as sharenting (which might not be criminal or harmful *per se*) can take different forms and be linked to a range of different (criminal or otherwise harmful) activities. Moreover, the criminal or otherwise harmful event originating by sharenting might be committed by different actors further complicating things: the sharenter, as we will see, is indeed only a part of the full picture.

Descriptive results

Temporal and geographical distribution

The newspaper articles taken into consideration cover the period from 2013 to 2021[7]. Newspapers and cases mentioned in them are geographically distributed over five continents (Europe, Asia, North America, Africa, Australia). The corpus of 32 articles comprised news reports and, mostly, feature articles, providing a total of 57 unique cases of different and nuanced degrees of sharenting leading to crimes or otherwise harmful events affecting minors.

The platforms

Among the 57 cases, Facebook was the platform involved in 25 cases, YouTube in 7 cases, Instagram in 21 cases, Twitter in 1 case, parents' blogs in 5 cases, parents' websites in 1 case, WhatsApp in 1 case, institutions' websites in 1 case. In the other cases, the articles referred to the platforms as 'social media' in a generic way.

The criminogenic aspects of these platforms were discussed in different ways in the media articles. For instance, in the case of YouTube, some articles highlighted a lack of legal protection for minors and ethical pitfalls mostly due to monetisation practices. Facebook was

[6] It is noted that the concept of script is originally derived from cognitive science, e.g., Abelson 1976; Nisbett and Ross 1980.

[7] These articles come from the following 23 newspapers: *Newsweek*, *CE Noticias Financieras English*, Independent, *Beijing Reviews*, Gulf News, *The Telegraph*, *The Guardian*, *SundayTimes (South Africa)*, *The Herald (Ghana)*, *CNN.com*, *Atlantic Online*, *LNP (Lancaster, PA)*, *MailOnline*, *The Irish Times*, *Daily Nation (Kenya)*, *Sydney Morning Herald (Australia)*, *Scottish Mail on Sunday*, *Daily News (South Africa)*, *The Straits Times (Singapore)*, *The Daily Telegraph (Australia)*, *Asia News Network*, *The Daily Telegraph (London)*, *Irish Independent*. The majority of reported cases are based in the UK (20), followed by the US (17), Australia (3), Singapore (3) and South Africa (3); Italy (2), Spain (2), Dubai (2) and Malaysia (2); and China (1), Ghana (1), and South Korea (1). Of course, these numbers should not be considered as an indication of the prevalence of cases in these geographical areas, as the data sampling strategy used does not allow us to draw any conclusion on this point. The articles have been published in 2019 (10), 2018 and 2021 (5 each), 2016 (4), 2013, 2014 and 2015 (2 each), 2017 and 2020 (1 each), and report about cases occurring in the same year or in previous years: 2016 (15), 2019 (11), 2013 and 2018 (5 each), 2021 (4), 2014, 2015, 2017 and 2020 (2 each), and 2009 (1). The date of the case was uncertain but we know it happened in between 2018 and 2021 in 8 cases.

frequently described as a social media platform that provides parents a sense of family, community support, and connection among relatives and friends. On the other hand, some articles depicted Facebook as a platform that creates a digital shadow for children over the years based on thousands of pictures posted by parents and this could threaten the social identity of affected children, particularly as they grow older. That said, Facebook was also described by several articles as a platform with a strong content moderation policy that is evident in the way it expedients the removal of inappropriate content that could harm both adults and minors. Instagram, on the other hand, was depicted as less safe and capable of exposing users to theft of images which could be reused for illegal purposes such as child pornography.

The sharenters and their motivations

In most cases, the sharenter was the mother (40), followed by both parents (12), the father (3), the mother and the sister (1), and the aunt (1). Often the mothers mentioned were media celebrities (actresses, writers or influencers) or 'mumfluencers' (that is, mothers who post about their experience as mothers from the onset of pregnancy). The fathers mentioned were also mostly celebrities or social media influencers.

While the sources used, of course, do not allow us to draw any firm conclusions about the sharenters' motivation, the articles suggest that the following are key motivational factors: parental pride in at least 23 cases, monetisation in at least 9 cases, social influence in at least 3 cases, social isolation in at least 2 cases, and the personal need to speak out in at least 2 cases. The motivations remain uncertain for the other cases. However, it is worth noting that some cases make it difficult to understand the balance between posting content for monetisation or for social influence purposes, and it appears that a combination of both contributes to the digital commodification of their children's identity, story and images. This is for instance the case of screen celebrities (those who hit celebrity status as a result of the attention given to them by mass media) and social media influencers who create a personal account on Instagram for their babies to allow fans to follow their lives and development. What is certain is that all sharing seemed deliberate and was done by social media influencers as part of their activities (in 21 cases), or by individuals using social media for non-professional purposes.

Crimes and social harms associated with sharenting and the perpetrators

In terms of the crimes against minors due to sharenting, the articles discussed: those initiated by the sharenters through the online dissemination of videos, photos, texts; and those orchestrated by other people who accessed the shared content. The crimes could be classified as follows: forms of antagonistic online behaviours (which include, *inter alia*, harassment and bullying, it was unclear form the news whether they met the legal standards for criminalisation or not in the relevant jurisdiction), present in 4 cases; child pornography (via pictures, even if originally not sexualised in nature, distributed with pornographic intent), present in 4 cases; and identity theft, present in 1 case. Additionally, 13 cases involved non-criminalised yet harmful unwanted digital exposure (i.e., cases were the minor made explicit s/he did not want to be exposed online, but the parent did it nonetheless); and 5 cases were about the digital commodification of the minor, reportedly leading to forms of child neglect when the exploitation was over.

Information available on the offender(s) was very scarce, with the exception of 9 cases where the 'bully' was the parent her/himself (purposely distressing the minor to gain more social media reaction), 1 case involving the child's followers, and 4 cases of 'stranger danger'.

Types of information shared

The sharing involved mostly pictures and videos, with only a few containing solely textual content. Information on victims was generally limited in the articles we analysed, but in terms of their demographic attributes, there was information suggesting that the risks of sharenting is not gender specific. It affects boys (as specified in 27 cases) and girls (as specified in 34 cases – the sum is higher than the total number of cases as, often, more minors were mentioned in the same case). Our analysis of the articles also suggests that sharenting is not age-related as it affects both babies and toddlers (as reported in 20 cases), older kids (in 15 cases), and teenagers (in 22 cases), although the older ones are particularly affected by cases of antagonistic online behaviours and unwanted digital exposure.

Reactions to victimisation associated with sharenting

The reported reactions to these harmful cases of sharenting are worth exploring, if only because they alert us to the variety of actors that are or can be involved in the process – each of them having the opportunity to intervene to prevent or mitigate the harms –, and the need for a more strategic and coherent response to the problem. This can be achieved if, for example, social media platforms educate users and establish clear protocols for identifying and reacting to sharenting risks. Meanwhile, our study found that, in the absence of clear strategies, reactions to victimisation were variegated and uncoordinated. They ranged from parents' public apologies to children and/or audience (2 cases), making contents private (i.e., change in privacy settings) (3), deleting contents/accounts by their own decision (8), deleting contents/accounts after court order (2), announcing that they would stop posting such content (5), posting only with minor's consent (2), calling the police after they discovered the use of children's pictures for pornography (1), reporting to the social media platform (3), warning against people who shared the pictures in an improper way (1). In one case, the social media platform (Facebook) took action against the improper use of children's pictures by parents (nudity). In another case, after the request of the minor, the adult refused to remove the picture from Facebook. Furthermore, several parents chose to ignore how the digital shadow and this digital exposure could affect their children in the future.

Crime script analysis: points of vulnerability in sharenting processes

To highlight specific points of vulnerability in sharenting processes, we created a master crime script (or 'metascript', see Leclerc 2017, as schematically represented in Figure 1) by assessing the information available in the single cases analysed. Because of the information used, it is an actual (rather than potential)-victim script (similarly to Smith 2017). Of course, our master script has a more limited role than scripts developed for 'simpler' criminal activities, where it is possible to comprehend how crime operates or needs to operate step-by-step, and is certainly more limited in its capacity to identify proper preventive measures. The traditional division into different scenes or functions (Clarke and Cornish 1985; Cornish 1994) used in many scripts between pre-activities, crime, and post-activities does not work very well with sharenting in general: depending on the nature of the specific sharenting case, criminal or otherwise harmful activities can manifest themselves in different stages of the process; they can start, continue or escalate in different moments; and they depend on the actions of different actors. Nonetheless, even if we broadened the level of analysis, the script tool can still offer a valid help in identifying the more vulnerable phases in sharenting practices, where interventions are missing, or proved ineffective for crime/harm prevention or harm mitigation.

Figure 1: A schematic representation of a master script for harmful sharenting practices

[Figure 1 about here]

As schematised in Figure 1, regardless of the specific script that might be followed in specific sharenting practices, a number of vulnerabilities (harm manifestations) can be observed at different levels, with effective interventions for the mitigation of those harms or the associated crimes being available only in a limited number of instances. Indeed, not only persistent, replicable, scalable and searchable (boyd 2010) manifestations of harm can occur in all the stages of the script, but there is also a severe lack of effective interventions to prevent, mitigate the effects of, or counter criminal and harmful events. Considering the digital and multidimensional nature of sharenting, the finding that vulnerabilities manifest themselves at various levels and the ineffectiveness of traditional intervention (for instance, criminal justice interventions on their own) are not new (as summarised in Lavorgna 2020: 188ff). Yet, the fact that only two out of the patterns identified in the master script ended with a satisfactory solution (that is, the harm stopped – in bold in Figure 1) is certainly revealing of the inability of existing mechanisms to deal with sociotechnical challenges such as sharenting.

Discussion

The process of data gathering itself and the data analysis have shown that, despite the increased attention to the media reported crime risks (e.g., identity theft, grooming, and sexual abuse) associated with sharenting, there seems to be a discrepancy between the media hype surrounding certain risks and the reported real-life occurrences of victimisation. This is the case despite the increasing scholarly and media attention to sharenting as a feature of contemporary digital parenting. We acknowledge that the scarce reporting of actual cases where sharenting actually led to the victimisation of minors does not imply that far more crimes or otherwise harmful activities linked to sharenting do not occur. Since sharenting generally happens in domestic settings and it is essentially a digital activity, it is likely that significant underreporting occurs (in line with Mihalic and Elliott1997; Thorneycroft and Asquith 2015; Martellozzo 2017; Lavorgna 2020).

The script analysis allowed us to identify contextual issues pertaining to the actual reported crimes. As such, our findings can help improve current understanding of the problem and how to develop preventative measures. To begin with, our study unravelled systemic vulnerabilities, specifically the lack of effective intervention by platform companies to prevent or address manifestations of harmful sharenting practices. This is likely to fuel more sharenting harms and crimes than are currently reported in the media. As such, despite our findings regarding the limited media reports of actual sharenting cases leading to victimisation, the perceived risks of sharenting should not be easily dismissed as unfounded. Further, it is important to pay attention to the social mechanisms which, by emphasising potential risks and dangers (Critcher 2009) for children and adolescents (Krinsky 2008), particularly online risks (Potter and Potter 2001), can awaken anxieties and fears (e.g., Cassell and Cramer 2008; Facer 2012; Cino and Dalledonne Vandini 2020). To better understand these social dynamics, there is the need of further media analysis in the future. Specifically, we hope that our exploratory analysis which sheds light on some aspects of criminological relevance affecting sharenting practices can serve as the basis to carry out further analyses detailing whether and how a moral panic may be occurring in the media framing of sharenting. We expect that this might imply the need to adapt the traditional version of the moral panic approach to meet the features and challenges of the digital field. Of particular relevance here are the tensions affecting the ‘digital custodian’ role of the sharers themselves, the tensions between creating a media hype by emphasising

newsworthy crime risks, and the recognition that certain forms of sharenting can indeed enable (at times subtle) forms of harms for young people. Additionally, the data sampling strategy used in this study comes with obvious limitations: further research should explore in more depth, publications at the national and local levels, and investigate more closely the sharenting features of diverse social media platforms.

Our study also provides additional contextual information about sharenting victimisation, and the information can help advance knowledge and policy intervention. Meanwhile, it is important to point out that sharenters are in a peculiar situation. First, in most of the cases observed, there is no malice in their intent. Instead, it may well be that they underestimate the risks, or seem unaware of the short and long-term harms that could originate from sharenting. In this regard, it is worthwhile to explicitly note that, in our study, there is no intent to blame the sharenters for risks and actual victimisation. As discussed elsewhere (Lavorgna et al. 2022), we acknowledge that users' agency is somehow constrained by structural factors and social media dynamics. Rather, through the *ProTechThem* project we want to understand better the social issues surrounding harmful forms of sharenting to raise awareness by unravelling these issues and how to address them.

The media reports we analysed discuss, to a certain extent, the existence of emotional harms (e.g., distress for having some personal information exposed), but the potential for other types of social or financial harms suffered by the minors, or risks to their current and future digital inclusion and citizenship, are not addressed. This suggests that these elements are not yet sufficiently part of the public debate, leaving the general public including sharenters poorly informed. With limited information about the digital hygiene needed to preserve clean and curated digital identities, the sharenters (and parents in particular, who traditionally have responsibilities of prevention and care – see Beck and Beck-Gernsheim 1995; Probert et al. 2009) appear unprepared in their new role as both gatekeepers and gate-openers of exposed identities (in line with Leaver 2020).

There is also the added issue of the collected and distributed nature of sharenting harms. Similar to what has been observed, for instance, in the context of image-based sexual abuse (that is, the non-consensual diffusion of intimate and/or sexual visual materials) (Pavan and Lavorgna 2021), the constitutive role of digital media in the creation and the specific dynamics of certain digital harms forces a shift beyond the traditional dichotomy of perpetrators-targets, as agency is often shared, relational, and distributed (see Lupton and Southertone 2021). In other words, apart from the sharenter and the minor, a variety of other human and nonhuman actors are involved, ranging from bystanders witnessing or contributing to crimes and harms to platforms' affordances and algorithms. The latter is driven by social media companies and their agendas. In particular, poor content moderation is a factor that can fuel the risks and harms of sharenting. But we recognise that, as stressed by Powell and colleagues (2018, 2020) among others, in many forms of digital harms technology cannot be considered a mere facilitator, as digital technologies are embedded in the larger social entity and operate at the intersection of human, social, and technical factors, all of which impact on both cultures and practices such as sharenting and the accompanying risks. Our study reveals how this occurs, that is, how sharenters engaged in the sociocultural practice of sharenting are aided by social media platforms with business models that emphasise monetisation and profit over ethical considerations such as effective content moderation for the protection of minors affected by the harms of sharenting. Therefore, policy makers interested in addressing the risk and harms of sharenting should consider the sociotechnical nature of such practices and pay attention to the need to address (all) the human, social and technical elements of such practices.

Conclusions

In our exploratory contribution, we offered a criminological perspective on sharenting practices, furthering the emerging multidisciplinary literature on this topic by analysing media reports to investigate whether and how media reported sharenting risks are commensurate with reports of actual crimes or other harmful activities against minors. We have shown that, despite the potential underreporting of cases where sharenting led to the victimisation of minors, there are systemic vulnerabilities in current sharenting practices that can cause the perpetration of harms. As such, even if there is paucity of reported cases where sharenting practices led directly to minors' victimisation, the risks of sharenting should not be easily under-estimated or dismissed altogether. There are indeed some genuine concerns requiring further attention.

Importantly, our findings regarding key contextual information about sharenting crimes can help raise awareness. The findings pertain to: the gender distribution of sharenters and victims which highlights mothers and female minors respectively; the role of financial and social benefits in driving sharenting practice; the tendency of sharenters to share images which in turn seem to attract more victimisation than textual information; and the lack of a coordinated strategy for addressing sharenting crimes.

By providing these insights, this study improves understanding of the crime risks and actual harms of sharenting, while providing a nuanced analysis of the reality of media's representations. While our study found gaps between reported risks and actual victimisation, it is worth noting that exploring media reports as we did in this study can help unravel evidence of exaggerated risks but can also reveal real crimes and harms, inform the public, and augment the development of preventive strategies. It could be argued that crime statistics are better sources of information. But the media have long been implicated in the problem of exaggerated and sensationalised reports than fuel public fears and anxieties (e.g., Jewkes 2015), indicating the influence the media can have on the public, and highlighting the importance of deep analysis of media reports to assess gaps between reported crime risks and actual victimisation. Besides, media reports can alert us to crucial contextual information necessary for developing preventive strategies. Examples include the degree to which different platforms are addressing criminogenic risks and specific points of vulnerability in sharenting processes. Whilst such information may not be useful for understanding the extent of the problem, it can yield insights that can inform public awareness and policy intervention.

We have integrated approaches stemming from very different theoretical premises: the constructionist approach linked to the analysis of media reports, and the opportunity theories at the basis of crime scripts. By doing so, we have offered a unique overview of sharenting practices, conceptualising sharenting as a more complex phenomenon than generally recognised, evidencing how it can display very different features and be linked to a variety of criminal or otherwise harmful events. From a public awareness perspective, informing about the multifaceted nature of sharenting can help demystify misguided beliefs which focus attention on some forms of harmful sharenting, and merely link its risks to the actions of professional content creators or influencers. From a policy intervention perspective, of course, our analysis operated at a high-level, and further analyses at narrower level of specificity are needed to better account for the identification of specific interventions. Nonetheless, our results can help initiate a discussion and identify priorities, including crime and harm prevention

mechanisms such as those targeted at modifying the human decisions preceding a harmful sharenting practice, perhaps in line with situational crime prevention teachings (Clarke 1992; Cornish and Clarke 2003; Freilich and Newman 2014). While a detailed discussion on potential policy interventions is beyond the scope of this article, it is important to stress that for such interventions to be successful, they have to operate at the intersection of human, social, and technical factors, as sharenting is a sociotechnical phenomenon combining both human actors (users, platforms' moderators) and nonhuman entities (the platforms and their automated tools).

References

Abelson RP (1976) Script processing in attitude formation and decision making. In: Carroll JS and Payne J (eds) *Cognition and social behavior.* Mahwah, NJ: Lawrence Elbraun Associates.

Agrafiotis I, Nurse JR, Goldsmith M, Creese S and Upton D (2018) A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity* 4(1): tyy006.

Ammari T, Kumar P, Lampe C and Schoenebeck S (2015) Managing children's online identities: How parents decide what to disclose about their children online. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, Seoul, Republic of Korea.

Barnes R and Potter A (2021) Sharenting and parents' digital literacy: an agenda for future research. *Communication Research and Practice* 7(1): 6-20.

BBC (2018) 'Sharenting' puts young at risk of online fraud. Available at: https://www.bbc.com/news/education-44153754.

Beck U and Beck-Gernsheim E (1995) *The normal chaos of love.* Cambridge: Polity Press.

Berger JA and Buechel E (2012) Facebook therapy? Why do people share self-relevant content online? Available at: https://ssrn.com/abstract=2013148.

Bezáková Z, Madle□ák A and □vec M (2021) Security Risks Of Sharing Content Based On Minors By Their Family Members On Social Media In Times Of Technology Interference. *Media Literacy and Academic Research* 4: 53-69.

Blum-Ross A and Livingstone S (2017) 'Sharenting', parent blogging, and the boundaries of the digital self. *Popular Communication* 15(2): 110-125.

Bonanomi G (2020) *Sharenting. Genitori e rischi della sovrapposizione dei figli online*. Milan: Mondatori.

Bossler AM and Berenblum T (2019) Introduction: new directions in cybercrime research, *Journal of Crime and Justice* 42(5): 495-499.

boyd D (2010) Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications. In: Z Papacharissi Z (ed) *Networked Self: Identity, Community, and Culture on Social Network Sites*. New York: Routledge, pp.47-66.

Brey P (2017) Theorising technology and its role in crime and law enforcement. In: McGuire MR and Holt TJ (eds) *Routledge Handbook of Technology, Crime and Justice*. Abingdon: Routledge, pp.17-34.

Briazu RA, Floccia C and Hanoch Y (2021) Facebook Sharenting in Mothers of Young Children: The Risks Are Worth It but Only for Some. *Technology, Mind, and Behavior* 2(4).

Brosch A (2018) Sharenting – Why Do Parents Violate Their Children's Privacy? *The New Educational Review* 54: 75-85.

Brown K, Ecclestone K and Emmel N (2017) The many faces of vulnerability. *Social Policy and Society* 16(3): 497-510.

Buchanan R, Southgate E and Smith SP (2019) 'The whole world's watching really': Parental and educator perspectives on managing children's digital lives. *Global Studies of Childhood* 9(2): 167-180.

Burnes D, DeLiema M and Langton L (2020) Risk and protective factors of identity theft victimization in the United States. *Preventive medicine reports* 17: 101058.

Button M, Blackbourn D, Sugiura L, Shepherd D, Kapend R and Wang V (2021) From feeling like rape to a minor inconvenience: Victims' accounts of the impact of computer misuse crime in the United Kingdom. *Telematics and Informatics* 64: 101675.

Cassell J and Cramer M (2008) *High tech or high risk: Moral panics about girls online.* Chicago: MacArthur Foundation Digital Media and Learning Initiative.

Chiu YN, Leclerc B and Townsley M (2011) Crime script analysis of drug manufacturing in clandestine laboratories: Implications for prevention. *British Journal of Criminology* 51(2): 355-374.

Choi GY and Lewallen J (2018) 'Say Instagram, Kids!': Examining Sharenting and Children's Digital Representations on Instagram. *Howard Journal of Communications* 29(2): 144-164.

Cino D and Dalledonne Vandini C (2020) 'Why Does a Teacher Feel the Need to Post My Kid?': Parents and Teachers Constructing Morally Acceptable Boundaries of Children's Social Media Presence. *International Journal of Communication* 14: 19328036.

Clarke RV (2008) Situational crime prevention. In: Wortley R and Mazerolle L (eds) *Environmental criminology and crime analysis*. Milton: Willan Publishing.

Clarke RV and Cornish D (1985) Modelling offenders' decisions: A framework for research and policy. *Crime Justice* 6: 147-185.

Clarke RV (1992) *Situational crime prevention. Successful case studies*. Albany, NY:Harrow and Heston.

Clough J (2015) Towards a common identity? The harmonisation of identity theft laws. *Journal of Financial Crime* 22(4): 492-512.

Cornish DB (1994) The procedural analysis of offending and its relevance for situational prevention. In: Clarke RV (ed) *Crime prevention studies no. 3*. Criminal Justice Press.

Cornish DB and Clarke RV (2003) Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. In: Smith MJ and Cornish DB (eds) *Crime prevention studies no.16*. Criminal Justice Press.

Coughlan S (2018) Sharenting puts young at risk of online fraud. *BBC News*. Available at: https://www.bbc.com/news/education-44153754.

Critcher C (2009) Widening the focus: Moral panics as moral regulation. *The British Journal of Criminology* 49(1): 17-34.

Dehghanniri H and Borrion H (2021) Crime scripting: A systematic review. *European Journal of Criminology* 18(4): 504-525.

Department for Digital, Culture, Media & Sport (2020a) Digital Identity: Call for Evidence. Available at: https://assets.publishing.service.gov.uk/government.

Department for Digital, Culture, Media & Sport (2020b) Digital Skills and Inclusion. Available at: https://digitalinclusion.blog.gov.uk.

Facer K (2012) After the moral panic? Reframing the debate about child safety online. *Discourse: Studies in the Cultural Politics of Education* 33(3): 397-413.

Feher K (2021) Digital identity and the online self: Footprint strategies – An exploratory and comparative research study. *Journal of Information Science* 47(2): 192-205.

Freilich JD and Newman GR (2014) Providing opportunities: A sixth column for the techniques of situational crime prevention. In Caneppele S and Calderoni F (eds) *Organised crime, corruption and crime prevention*. Cham: Springer.

Geddes L (2019) Consider your child future before you share. *New Scientist* 242: 24-25.

Golladay K and Holtfreter K (2017) The consequences of identity theft victimization: an examination of emotional and physical health outcomes. *Victims & Offenders* 12(5): 741-777.

Hancock H (2021) The impact of the image on personal life: is current law out of focus? *Journal of Media Law* 13(1): 54-80.

Hollway W and Jefferson T (1997) The risk society in an age of anxiety: situating fear of crime. *British journal of sociology* 48(2): 255-266.

Holt TJ and Turner MG (2012) Examining risks and protective factors of on-line identity theft. *Deviant Behavior* 33(4): 308-323.

Jewkes Y (2015) *Media and Crime*. London: Sage.

Jorge A, Marôpo L, Coelho AM and Novello L (2021) Mummy influencers and professional sharenting. *European Journal of Cultural Studies*. doi:10.1177/13675494211004593.

Kloess JA, Hamilton-Giachritsis CE and Beech AR (2019) Offense processes of online sexual grooming and abuse of children via internet communication platforms. *Sexual Abuse* 31(1): 73-96.

Kolaczek G (2009) An approach to identity theft detection using social network analysis. *First Asian Conference on Intelligent Information and Database Systems.*

Krinsky C (ed) (2008) *Moral panics over contemporary children and youth*. Farnham: Ashgate Publishing.

Lavorgna A (2014) Wildlife trafficking in the Internet age: The changing structure of criminal opportunities. *Crime Science* 3(5):1-12.

Lavorgna A (2015) The online trade in counterfeit pharmaceuticals: New criminal opportunities, trends, and challenges. *European Journal of Criminology* 12(2):226-241.

Lavorgna A (2020) *Cybercrimes: Critical issues in a global context*. London: Bloomsbury.

Lavorgna A (2021a) *Information pollution as social harm: Investigating the digital drift of medical misinformation in a time of crisis*. Bingley: Emerald Publishing.

Lavorgna A (2021b) Looking and crime and deviancy in cyberspace through the social harm lens. Leighton PS, Wyatt T e Davies P (eds.) *Handbook of Social Harm*. Basingstoke: Palgrave, pp.401-420.

Lavorgna A, Tartari M and Ugwudike P (2022) Criminogenic features of social media platforms: the case of harmful sharenting practices. *European Journal of Criminology*, https://doi.org/10.1177/14773708221131659.

Lazard L, Capdevila R, Dann C, Locke A and Roper S (2019) Sharenting: Pride, affect and the day-to-day politics of digital mothering. *Social and Personality Psychology Compass* 13(49): e12443.

Leaver T (2020) Balancing privacy: Sharenting, intimate surveillance, and the right to be forgotten. *The Routledge Companion to Digital Media and Children*. London: Routledge, pp. 235-244.

Leclerc B, Wortley R and Smallbone S (2011) Getting into the script of adult child sex offenders and mapping out situational prevention measures. *Journal of Research in Crime and Delinquency* 48(2): 209-237.

Leclerc B (2017) Script analysis and the SCRIPT acronym. In: Leclerc B and Savona EU (eds) *Crime Prevention in the 21st Century. Insightful Approaches for Crime Prevention Initiatives*. Cham: Springer.

Lupton D and Southerton C (2021) The thing-power of the Facebook assemblage: Why do users stay on the platform? *Journal of Sociology* 57(4) :969-985.

Martellozzo E (2017) Online sexual grooming. Children as victims of online abuse. In: Martellozzo E and Jane EA (eds) *Cybercrime and its victims*. London: Routledge.

Mihalic SW and Elliott D (1997) If violence is domestic, does it really count? *Journal of Family Violence* 12(3): 293-311.

Minkus T, Kelvin L and Ross KW (2015) Children seen but not heard: When parents compromise children's online privacy. *Proceedings of the 24th international conference on World Wide Web.*

Monahan T (2009) Identity theft vulnerability: neoliberal governance through crime construction. *Theoretical Criminology* 13(20): 155-176.

Moreto WD and Clarke RV (2013) Script analysis of the transnational illegal market in endangered species. Dream and reality. In: Leclerc B and Wortley R (eds) *Cognition and crime: offender decision-making and script analysis*. London: Routledge.

Moskovitch R, Feher C, Messerman A, Kirschnick N, Mustafic T, Camtepe A, Lohlein B, Heister U, Moller S, Rokach L and Elovici Y (2009) Identity theft, computers and behavioural biometrics. *IEEE International Conference on Intelligence and Security Informatics.*

Muncaster P (2019) Peace Sign Pics could give hackers your fingerprints. *InfoSecurity*, January.

Nisbett RE and Ross L (1980) *Human inference: strategies and shortcomings of social judgment.* Upper Saddle River, NJ: Prentice-Hall.

Nottingham E (2019) 'Dad! Cut that part out!' Children's rights to privacy in the age of 'generation tagged': sharenting, digital kidnapping and the child micro-celebrity- In: Murray J, Swadener B and Smith K (eds) *International Handbook of Young Children's Rights*. London: Routledge, pp.183.191.

OFCOM (2017) Box Set Britain: UK's TV and online habits revealed. Available at: https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2017/box-set-britain-tv-online-habits.

Orlando J (2017) How over-sharenting can harm your kids. *Nurture* 51(1): 14-15.

Ouvrein G and Verswijvel K (2019) Sharenting: Parental adoration or public humiliation? A focus group study on adolescents' experiences with sharenting against the background of their own impression management. *Children and Youth Services Review* 99: 319-327.

Papaioannou T, Tsohou A and Karyda M (2020) Shaping Digital Identities in Social Networks: Data Elements and the Role of Privacy Concerns. *Lecture Notes in Computer Science,* 11980.

Pavan E and Lavorgna A (2021) Promises and pitfalls of legal responses to image-based sexual abuse. Critical insights from the Italian case. In Powell A, Flynn A e Sugiura L (eds.) *Handbook on Gender, Violence and Technology*, pp. 545-564.

Potter RH and Potter LA (2001) The internet, cyberporn, and sexual exploitation of children: Media moral panics and urban myths for middle-class parents? *Sexuality and Culture* 5(3) :31-48.

Potter A and Barnes R (2021) The 'sharent' trap: parenting in the digital age and a child's right to privacy. In: Holloway D, Wilson MA, Murcia K, Archer C and Stocco F (eds) *Young children's rights in a digital world: Play, design and practice*. Cham: Springer, pp. 283-297.

Powell A, Stratton G and Cameron R (2018) *Digital criminology. Crime and justice in digital society*. New York: Routledge.

Powell A, Flynn A and Henry N (2020) Sexual Violence in Digital Society: Human, Technical and Social Factors. In: Holt T and Leukfeldt R (eds) *Understanding the Human Factor of Cybercrime*. New York: Routledge.

Probert R, Gilmore S and Herring J (eds) (2009) *Responsible parents and parental responsibility*. London: Bloomsbury Publishing.

Roberts LD, Indermaud D and Spiranovic C (2012) Fear of cyber-identity theft and related fraudulent activity. *Psychiatry, Psychology and Law* 20(3): 315-328.

Saner E (2018) The 'sharent' trap – should you ever put your children on social media? *The Guardian*. Available at : https://www.theguardian.com/lifeandstyle/2018/may/24/sharent-trap-should-parents-put-their-children-on-social-media-instagram.

Sanders R (2020) Digital inclusion, exclusion and participation. Available at : https://www.iriss.org.uk/resources/esss-outlines/digital-inclusion-exclusion-and-participation.

Siibak A (2019) Digital parenting and the datafied child In: Burns T and Gottschalk F (eds) *Educating 21st Century children: emotional well-being in the Digital Age*. Paris: OECD Publishing.

Siibak A and Traks K (2019) The dark sides on sharenting. *Catalan Journal of Communication & Cultural Studies* 11(1): 115-121.

Smith M (2017) Expanding the script analytic approach using victim narratives: learning about robberies of taxi drivers from the drivers themselves. In: Leclerc B and Savona EU (eds) *Crime Prevention in the 21st Century. Insightful Approaches for Crime Prevention Initiatives*. Cham: Springer.

Steinberg SB (2017) Sharenting: Children's Privacy in the Age of Social Media. *EMORY L.J.* 66(839).

Steinmetz KF (2021) The Identification of a Model Victim for Social Engineering: A Qualitative Analysis. *Victims & Offenders* 16(4): 540-564.

Taaffe O (2019) *Banking on Change: the development and future of financial services*. Medford, MA: Wiley.

Thorneycroft R and Asquith NL (2015) The dark figure of disablist violence. *The Howard Journal of Criminal Justice* 54(5): 489-507.

Tremblay P, Talon B and Hurley D (2001) Body switching and related adaptations in the resale of stolen vehicles. *British Journal of Criminology* 41(4): 561-579.

Verswijvel K, Walrave M, Hardies K and Heirman W (2019) Sharenting, is it a good or a bad thing? Understanding how adolescents think and feel about sharenting on social network sites. *Children and Youth Services Review* 104: 104401.

Wachs S, Mazzone A, Milosevic T, Wright MF, Blaya C, Gámez-Guadix M and O'Higgins Norman J (2021) Online correlates of cyberhate involvement among young people from ten European countries: An application of the Routine Activity and Problem Behaviour Theory. *Computers in Human Behavior* 123: 106872.

Walklate S (2011) Reframing criminal victimization: finding a place for vulnerability and resilience. *Theoretical Criminology* 15(2): 179-194.

Williams ML (2016) Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. *British Journal of Criminology* 56(1): 21-48.

Williams-Ceci S, Grose GE, Pinch AC, Kizilcec RF and Lewis NA (2021) 'Combating sharenting: Interventions to alter parents' attitudes toward posting about their children online. *Computers in Human Behavior* 125: 106939.

Appendix A – Coding framework

CODE	SUBCODE
Year	2013-2021
Type of social media used	Facebook, YouTube, Instagram, Twitter, WhatsApp
Type of crime	Antagonistic online behaviours; child pornography; identity theft; child neglect
Type of harm	Unwanted digital exposure; digital commodification; other
Stages	Preparatory activities; modus operandi; post-crime/harm activities
Sharenter	E.g., mother, father, "parent" in general, teacher, carer, others acting *in loco parentis*
Other sharenter's info	E.g., gender, age, ethnicity, social status, including ways in which they are represented
Type of sharenting	E.g., unintentional vs deliberate
Explicitly state sharenter's motivation	E.g., the sharenter states why s/he is posting the content

Represented sharenter's motivation represented by the journalist, if any	E.g., money, pride, insecurity, social media influence (e.g., to increase likes, followers).
Child/children who are object of sharenting	E.g., number, their relationship with the sharenter, age, gender, ethnicity
Offender/harasser	E.g., number, their relationship with the sharenter or the minor, age, gender, ethnicity
Type of information shared	E.g., video; picture; text
Responses and reactions	E.g., by law enforcement, social media company, social media moderator/administrator, friends and family, other

Figure 1: A schematic representation of a master script for harmful sharenting practices