This manuscript has been accepted for publication in the *Journal of the Association for Information Systems*, 9 Oct 2020.

ONLINE CHILD SEXUAL EXPLOITATION: A NEW MIS CHALLENGE

Dionysios S. Demetis
Centre for Systems Studies, Hull University Business School, U.K
d.demetis@hull.ac.uk

Jan Kietzmann
Gustavson School of Business, University of Victoria, Canada
jkietzma@uvic.ca

Abstract

This paper deals with the difficult yet increasingly important MIS phenomenon of online child sexual exploitation (online CSE). Through the use of secondary and publicly available data from the Federal Bureau of Investigation (FBI), as well as primary data from a cybercrime police unit in the United Kingdom, this study takes a grounded theory approach and organises the role that technologies and social actors play in shaping online CSE. The paper contributes to IS theory by providing a consolidated model for online CSE, which we label as the Technology and Imagery Dimensions Model (TIDM). This combines the staging of the phenomenon and the key dimensions that depict how the use of technology and imagery both fuels and defuses the phenomenon. In informing the construction of the model, the paper extracts, organises, and generalises the affordances of technology and discusses the role of information systems in detecting online CSE.

Keywords: online child sexual exploitation, CSE, child protection, cybersecurity, cybercrime, grounded theory

ONLINE CHILD SEXUAL EXPLOITATION: A NEW MIS CHALLENGE

INTRODUCTION

The exploitation of children is a disturbing topic with serious social repercussions (Carr, 2013). Sadly, the diffusion of digital technologies has been misused to fuel an ecosystem of activities that victimize children. Despite efforts from cybercrime police to counter such phenomena, one of the most serious forms of abuse online is *online child sexual exploitation* (hereinafter "online CSE") (Jalil, 2015). This must be distinguished conceptually from online SE (the online sexual exploitation of adults) that has other socio-economic vulnerability factors (e.g. bereavement, social exclusion, homelessness, immigration), stronger financial fraud elements (e.g. defrauding elderly of their pensions) and where image-solicitation is dwarfed by the adult porn industry (Miller and Veltkamp, 1998). In this paper, we concentrate solely on online CSE.

Online CSE includes activities on the Internet (e.g. online pornography) but can also be connected to serious contact offences including rape, kidnapping, trafficking and murder. Yet, despite its social significance and the multifaceted role of technology in both enabling and constraining the phenomenon, Information Systems (IS) as a field has not thus far engaged with the study of online CSE. The study presented here deconstructs the connections between information and communication technologies (ICTs) and online CSE and explores these connections primarily within the organisational context of a Cyber-Crime Unit (CCU) in a local Police force in the United Kingdom. The article contributes to our theoretical understanding of the phenomenon by developing a staging model for online CSE, relating it to an organisational

context, and by extracting, organising, and generalising the affordances of technology in enabling and constraining the goal-oriented actions of offenders and cybercrime police.

The remainder of this article is structured as follows: the second section reviews related work while the third section presents the methodology of the study. The fourth section presents our findings in relation to staging, and the fifth section presents our main findings around the use of IS at the CCU. In that context, affordances are extracted and generalised. The final section offers some conclusions about the nature of the phenomenon and its evolution, and sets out future research possibilities and indeed, research responsibilities for IS scholars.

RELATED WORK

One of the key dynamics of online CSE is its staggering growth in the past two decades (Breeden and Mulholland, 2006). For example, in the United States, a 988% increase in arrests was witnessed between 2000 and 2006 (Mitchell *et al.*, 2010). More recent work points to a global viral-like expansion as the Internet has enabled increased interconnectivity (Calcara, 2013). In the UK, a 700% increase has been recorded in the number of online CSE referrals to the National Crime Agency between 2013 and 2019 (NCA, 2019). Meanwhile, the security-oriented significance of online CSE is evident from the UK's national security strategy. Online CSE is included as part of cybersecurity risk that - along with international military crises, pandemics, and terrorist incidents is classified as a Tier 1 threat to the country (UKGov, 2015).

Despite the recognised importance of (and need for) more research into online CSE, the only tangential IS reference we could find comes from Lee's (2015) editorial as President of the Association of Information Systems (AIS). Lee mentioned that the "Council of the AIS has

adopted a grand vision of an ICT-Enabled Bright Society, with the goal of preventing undesirable activities on the Internet". The Internet has "become a minefield of crime" (p.iii) where "child protection" (p.ix) has become a major concern. In light of a lack of IS-literature dedicated to online CSE, we draw the main technology-oriented affordances of online CSE from other disciplines. This allows us to highlight the key characteristics of the phenomenon and to achieve a pre-understanding of online CSE. We use the concept of *affordances* in order to help us weave a cross-disciplinary thread that will build up that pre-understanding, but also, in order to organise the later sections of the analysis.

Affordances

The concept of an affordance originates in Gibson's work in the context of his ecological approach to visual perception (1977). Gibson used the concept of *affordance* to fence off the idea that humans (and other living beings) orient to objects in their environment and that the interaction between humans and objects creates possibilities for action (i.e. affordances). For example, a "rock may have the affordance, for a reptile, of being a shelter from the heat of the sun; or, for an insect, of concealment from a hunter" (Hutchby, 2001, p. 447). The appeal of this general form of interaction between any species and objects in their environment, as well as the multiplicity of possibilities that objects open up for interaction, has led to the transposition of the concept of affordances in IS research; in it, the materiality of technological artifacts has been perceived as giving rise to possibilities for user-computer interaction, or more generally, interaction between a user and any given IT-related artifact (which could be a software application, a social network, a set of features, etc).

Thus, the use of the idea behind affordances has been deployed in IS research in a number of ways and framed as "the possibilities for goal-oriented action afforded to specified user groups by technical objects" (Markus and Silver, 2008, p. 622). As Leonardi points out, the key idea is that objects have properties, or features in the context of information technology, and users perceive the utility of these (i.e. what they afford) through user-computer interaction; naturally, one technology can support multiple affordances (Leonardi, 2013). However, affordances should not be perceived as freely variable. For example "while a tree offers an enormous range of affordances for a vast variety of species, there are things a river can afford which the tree cannot, and vice versa" (Hutchby, 2001, p. 447). Hutchby (2001) also argues that technological materiality is both *constraining* and *enabling.* This distinction between enabling/constraining affordances can be thought of as the functional dimension of affordances and a very useful way of both categorising and reflecting on affordances. But affordances are not only functional; they are also *relational* (Hutchby, 2001) in the sense that affordances are different from one group of users to another and that different observers/users will perceive different affordances. In saying that "affordances can both enable and constrain" (Volkoff and Strong, 2013, p. 823), relationality is important; in an example of a fallen log in the woods, "someone wanting to walk along a path may consider a *barricading affordance constraining*, whereas someone wishing to prevent passage would consider it *enabling*" (Volkoff and Strong, 2013, p. 823). Thus, it is important to state that the "affordances of an artefact are not things which impose themselves upon humans' actions with, around, or via that artefact. But they do set limits on what it is *possible* to do with, around, or via the artefact. By the same token, there is not

one but a variety of ways of responding to the range of affordances for action and interaction that a technology presents" (Hutchby, 2001, p. 453). This relationship is both open and bounded.

Using these ideas, Leonardi develops a classification of affordances as individualised, collective, and shared (Leonardi, 2013): an *individualised affordance* is an affordance that someone enacts when using a technology's features but that affordance is not common to his group*;* a *collective affordance* signals differential-use and is collectively created by members of a group (e.g. a final output is created by individuals that work on their own, usually specialised, tasks); a *shared affordance* denotes *similar use* where individuals in the group use technology in roughly the same ways. However, we would like to highlight a further distinction. While offenders engage in deliberate goal-oriented actions through which technology enables online CSE, at the same time, there is non-offender-oriented use of technology that might enable online CSE, but unwittingly; these would constitute *misperceived affordances* based on Gaver (1991). Misperceived affordances, in the context of online CSE involve affordances that are *not perceived* by a user group although they do exist (e.g. the online dissemination of photographs by parents). Overall, the various conceptualizations of affordances assist us in both organising the pre-understanding of the phenomenon, and driving the discussion of online CSE forward.

The enabling and constraining affordances of technology in online CSE

Online CSE has been studied from several perspectives. Legal (Barnard-Wills, 2012), criminological (Tener, Wolak and Finkelhor, 2015) and psychiatric (Quayle and Newman, 2015) studies offer important insights. For example, Elliott and Beech (2009) find many interlocking neuropsychological aspects that describe offender behaviour: emotional problems, social

difficulties, cognitive distortion and deviant behaviour. Others focus around building typologies of online offenders themselves and classify them into two major categories: *traders* (where peer-to-peer (P2P) networks enable users to traffic child pornography online) and *travellers* (where social media and other forms of interaction enable offenders to engage in online discussions and to coerce children for sexual purposes) (Alexy, Burgess and Baker, 2005). The behaviour of young users is considered as an important part of the problem. For instance, Wells and Mitchell (2008) found that the routine connectivity, afforded to children who exhibit aggressive behaviour online, make it twice as likely for these children to become victimised. In assessing the experiences of online victimization by using routine activity theory, Marcum, Ricketts, and Higgins (2010) described how children become suitable targets, mostly by providing personal information online. The relationship between parents and young internet users is also studied by psychologists that explore how these affect the structure of online communications (McCarthy, 2010).

Perpetrators and online CSE

With the Internet allowing paedophiles to find each other, scholarly work has highlighted the significant role of child-abuse *imagery* and the creation of underground markets (Eisenstein, 2013). However, while different ways have been proposed to classify offenders (Tener, Wolak and Finkelhor, 2015), there is general agreement (Bartels and Merdian, 2016) that they can be differentiated between: a) *contact sex offenders* (who are enabled by technology to pursue and lure their victims online with the intent to cause physical harm and crimes like child sex-slavery and trafficking (Akullo, 2012)) and, b) *purely online sex offenders* that confine their actions to

the online space (Alexy, Burgess and Baker, 2005). Such classifications have a criminological orientation however and they do not explain the process or the stages through which either type of offenders is enabled by technology to commit online CSE. As Malesky (2007) notes, purely online offenders may still engage in serious criminal activities including online extortion and distribution of child pornography through P2P networks. Even though 62% of cases in the US involve possession-only offenses, child pornography is seen as part of a larger pattern of offending behaviour where the role of technology in it is complex (Owens *et al.*, 2016).

With most of the focus being placed on offender classifications per se, there is an important gap in exploring the broader affordances of technology in online CSE (both enabling and constraining). Most of the literature around online CSE focuses on behaviours and motivations and not as much on the constraining affordances and the contextual organisational aspects that would shape them. However, some work in P2P networks does shed some light upon the intensity with which online communities of paedophiles share content. The study of Wolak, Liberatore and Levine (2014) on Gnutella measured one year's worth of traffic, with the measurements focused on already known pornographic images of children that had a registered digital footprint from previous police investigations (each image was uniquely hashed). By collecting the individual IP addresses of users, they found that 244,920 U.S. computers shared 120,418 unique child pornographic files. A surprising finding was that the majority of users were 'contributing' a few images and less than 1% 'contributed' more than 100 images. This high-volume/low-level activity of images shows just how widespread the phenomenon has become. It further emphasizes that even though it is clear that technology enables offenders to share child pornography, the specific function of imagery behind online CSE seems to occupy a more

complex role. While the existing literature seems to portray imagery as part of the end goal of the phenomenon, due to its extent and interference, nuances of imagery play a more foundational role in fuelling/defusing the phenomenon. For example, what are the challenges related to imagery that are faced by cybercrime police in preventing, detecting, and pursuing the offenders?

Victims, Digital Imagery and online CSE

The importance of deconstructing the role of technology is perhaps most evident in the conceptual centrality that digital imagery occupies in online CSE. In laying out the potential ICT research agenda for online CSE, Hillman et al. (2014) do mention that we need to understand how technology is being used by criminals in relation to imagery since offenders are enabled by imagery and technology in varying ways to achieve different goals. In challenging the role of imagery, we also see it as a dimension of interference for online CSE that occupies different contexts, institutional efforts, organisational processes within teams (e.g. in cybercrime police) and shapes enabling/constraining, or misperceived affordances. Since the role of imagery is also critical from a detection perspective, cybercrime police will use different information systems in order to constrain online CSE, while the mechanism of that containment takes place through imagery. However, a recognition of the combined significance of the role of technology in online CSE imagery and the sociotechnical challenges that can be found in a cybercrime organisational context is largely absent. Confining the phenomenon cannot be realised without a deeper understanding of how conditions in tackling cybercrime at the organisational level take shape via different affordances.

Unsurprisingly, the way offender-oriented technology-use enables online CSE is also linked to how the victims approach technology as users. Behaviourally, scholars point out that technology-use for children has become a significant part of their lives and youngsters will experience online relationships first, even before they engage in real ones (Dowdell and Bradley, 2010). This exposes them to stalking, harassment and bullying (Smith, 2014), or even to paedophiles. Unfortunately, youngsters do not usually understand the full spectrum of risks until it is too late (Guan and Huck, 2012). Alas, parents can be victims, too, as they suffer a great deal if their children are targeted. But parents play another significant role in online CSE. As we will discuss, when parents post images of their children, they provide fodder for predators who trawl social networking sites to harvest imagery (Richards, 2015). As Australia's Children's e-Safety Commissioner, Alastair MacGibbon notes, there are multiple challenges that come about as paedophiles will edit images to make them look as if they are pornographic. They will sexualize the material and conduct highly explicit user discussions by reposting them in paedophilia websites (Battersby, 2015). Based on Richards (2015), as much as half of the material found on paedophile-websites is sourced or stolen from parents innocently posting images of their families online. This also creates a sense of "permanence once abusive images have been distributed online" and can be trafficked in perpetuity (von Weiler, Haardt-Becker and Schulte, 2010, p. 211). The role of imagery (including video) is critical for both fuelling online CSE (Quayle and Newman, 2015) and for detecting it (Wolak, Liberatore and Levine, 2014). However, there is considerable fragmentation in looking into this problem and a need to move towards more integrative approaches (Livingstone, 2008). We summarise the key preceding insights in Table 1

below while we include the key characteristics for the problematisation of the phenomenon (following Alvesson and Sandberg (2011) in Appendix 1).

Technology artefacts and affordances	Fueling the phenomenon	Authors	Defusing the phenomenon	Authors
P2P Networks *Exchanging imagery*	*Offenders* exchange child-abuse imagery in underground markets, often in high-frequency/low-volume transacting of child pornographic imagery	Elliott and Beech (2009) (Quayle and Newman, 2015) Malesky (2007) (Eisenstein, 2013) Wolak, Liberatore and Levine (2014)	*Cybercrime Police* will attempt to monitor networks to identify offenders and image exchanges; networks can also be monitored to give us a sense of volume of already known images in circulation	Wolak, Liberatore and Levine (2014) (Battersby, 2015)
Social media *Establish online relationships*	*Offenders* approaching children for coercion/exploitation	(Alexy, Burgess and Baker, 2005) Wells and Mitchell (2008) (McCarthy, 2010) (Smith, 2014) (Dowdell and Bradley, 2010) (Guan and Huck, 2012) (Richards, 2015)	*Technology Companies* and *Cybercrime Police* will attempt to detect imagery and block online CSE. A more integrative approach in tackling online CSE is important. *Children's attitudes* towards what they can and cannot share in social media can help prevent their exposure and exploitation; a better understanding of the full spectrum of risks is needed	(Wolak, Liberatore and Levine, 2014) (Livingstone, 2008) (Guan and Huck, 2012)
	Children become suitable targets through the unwitting provision of personal information online			
	The relationship between *parents* and *children* affects the structure of online communications			
	Children's attitudes towards online relationships exposes them to dangers that can culminate to online CSE			
	Parents' posting images of their children can provide raw material for exploitation, manipulation, sexualisation			

Table 1: A brief summary of the pre-understanding of the phenomenon and its basic affordances

Despite the variety of approaches used to study online CSE and the different classifications abstracted from criminology and other disciplines, there is an important gap in delineating the technology-oriented aspects of online CSE. From the preceding discussion, it

becomes evident that while it is known that technology enables online CSE and that it also constrains it, a deeper analysis into how that takes place is missing. It is not clear how the activities that offenders undertake by using technology are connected with each other and how the centrality of imagery affects different stages. Thus, it becomes clear that whatever IS theoretical development is being pursued, this must be sensitive, theoretically, to the inclusion of imagery and a deconstruction of the stages through which such use is being facilitated. Imagery is also important in delineating how the UK cybercrime unit (CCU) tackles the phenomenon so we expect a number of affordances (enabling and constraining) to be focused around imagery.

While studies similar to Wolak et al (2014) monitor Peer-to-Peer networks, no IS study has been conducted to explore the role of information systems in tackling online CSE within an organisational context. In order to address these gaps, while accepting the central role of imagery for both offenders and for those tasked with its prevention and detection, we focus on deconstructing the relationship between online CSE and technology by: a) taking account the centrality of imagery and delineating the process through which imagery is being used, b) extracting the enabling and constraining affordances of technology in online CSE, informed also by an organisational context of a UK cybercrime unit (CCU) in UK police.

How does technology and imagery enable and constrain online CSE for offenders and the CCU? How can the process of online CSE be delineated if we take imagery to affect different stages of the process? In order to elucidate these aspects, we focus on the IS implications of the phenomenon in the organisational context of cyber-crime unit of a UK police authority.

METHODOLOGY

As we seek to understand online CSE from an IS perspective, we use both secondary data (from FBI cases prosecuted in the US) and primary empirical data (from a cybercrime unit in the UK) in order to address aspects a) and b) as mentioned in the previous section. Given the close cooperation between the US and the UK, the direct reporting of IP addresses from the US to the UK on UK-based suspects and the multi-jurisdictional nature of the online phenomenon, a US/UK perspective can capture online CSE challenges in a more meaningful way. Also, given that offenders in the US and the UK use the same social media and other platforms operated by US-tech-companies, and taken that offenders across borders collaborate in underground forums (Quayle and Newman, 2015), a degree of homogeneity in online CSE can be expected (at least in how technology and imagery would enable or constrain it). In a crime conducted mostly in an online environment, jurisdiction becomes less important in the phenomenon's emergence, though it remains critical for prosecution and committing resources to its prevention and detection.

The research follows an interpretivist epistemology (Walsham, 1995; Klein and Myers, 1999) and an inductive reasoning underpinned by a grounded theory approach (Glaser and Strauss, 1967; Strauss and Corbin, 1998). Grounded theory allows us to develop both the context behind our phenomenon and strive for explanation (Orlikowski, 1993). The goal is to move towards theoretical development (Corbin and Strauss, 2007, p. 107) as "current understanding of the phenomenon is severely limited due to a lack of theoretical and empirical research in the area" (Martin, 2014, p. 96). Thus, theory is generated during research and grounded in data from the field, especially in the "actions, interactions and social processes of people" (Creswell, 2013, p. 84). In these inductive studies, the construction of theories or conceptual models occurs through the structured analysis of data (Martin and Turner, 1986).

Based on the goals of the research and as theoretical sensitivity is increased when informed by the literature (Glaser, 1978, p. 3), we have adjusted the theoretical sensitivity of our grounded theory approach by focusing on the process through which imagery is being used in online CSE (since the centrality of imagery is pivotal and used by offenders at the core of the phenomenon and cybercrime police for detection purposes). Furthermore, we extract the relevant affordances of technology in online CSE (Gibson, 1977; Markus and Silver, 2008; Volkoff and Strong, 2018). This helps us organise, develop, and abstract our understanding of the phenomenon and reflect on the corresponding affordances of technology. With the exception of the significance of imagery that we knew was critical for the phenomenon itself, we held no preconceived ideas as to the development of our framework. The combination of both the public cases and the interviews conducted (Table 2) led to rich data.

In the first phase of our research (Phase 1), we built up our staging model that we abbreviate as TIDM (Technology & Imagery Dimensions Model) from 37 public cases of the U.S. Federal Bureau of Investigation (FBI)[1]. In the first coding stages, the active engagement with the data led to the some key categories on how technology was used for: i) image solicitation or distribution, reflecting the centrality of imagery in online CSE as described in the literature review, ii) social network participation (or other channel of use), reflecting the ways in which social networks are being used by both offenders and victims, iii) *how* criminals used technology to facilitate online CSE, and iv) user implications. A sample of a case is shown in

[1] This sample was selected on the basis of secured convictions with the cases corresponding to FBI field offices in Miami, Detroit, San Francisco, Oklahoma City, Philadelphia, Washington DC, San Diego, Baltimore, Los Angeles, New York, Detroit, and Chicago.

Appendix 2 while a sample of 5 coded cases is shown in Appendix 3. Re-coding and category malleability was shaped through visual collaborative mind-mapping; we used visual data coding through a mind-mapping web-application (Coggle) as it allowed us to connect and collaborate, discuss the categories created while its interactive visualizations allowed us to explore the underlying data. This iterative process, whereby data is being compared with emerging categories/codes, data is compared with data, and codes with codes is known as *constant comparison.* Achieving constant comparison visually allowed us to develop more interesting interconnections (Charmaz, 2014), to benefit from a higher degree of malleability by moving branches of the codes around, to re-examine data and to combine or enrich the categories. This process continued into Phase 2 as well. We portray different time slices of this process in Appendix 3. This process allowed us to go through the open, axial and selective coding stages and the Coggle's timeline features allowed us to go back in time, explore modifications and rebuild our model. We stopped adding further FBI cases when we no longer made significant changes to the TIDM model, signalling that saturation was achieved.

In the second phase of our research (Phase 2), we sought to connect and contextualize our TIDM model in an organisational context, gain a broader understanding of online CSE and extract the different affordances. For these reasons, we conducted primary data collection at a specialist CyberCrime Unit (CCU). Detection attempts revolve around different uses of technology and imagery, which helped us anchor our UK fieldwork at the CCU onto the TIDM model. In our UK primary data collection, we interviewed 14 specialists and participated in four observation sessions with a total of 64 participants. We included the details of interviewees and the observation from the Cyber Crime Unit and from other organisations in Table 2. The

interviews were open-ended so as to capture a wide spectrum of technology and imagery-related aspects in line with our grounded theory approach. The average duration of interviews was 1.5 hours; observation sessions lasted two hours in the context of the online safeguarding children boards at the local council (with the exception of one that lasted 4.5 hours). Due to the sensitivity of the domain, no audio was requested and interviewees were made aware that all names/institutions would be anonymized. Notes were taken during the collection of empirical data and refined straight-after for completion. No victim imagery was shown or accessed by the researchers throughout this study; no online access was granted to specialised online tools at all; all of our primary data comes solely from interviews with experts or expert discussions.

The integration of the data from Phase 2 allowed us to combine our TIDM model with organisational considerations from an IS perspective. It also reinforced the categories created from the FBI cases while allowing us to refine the dimensions of imagery and technology as illustrated in Figure 1. The rich data/notes from the interviews and the insights from the FBI cases were first organised in separate word documents and then combined for integration, sorting, writing memos and reflections on interviewee comments, as well as refining the conceptual categories before extracting a complete list of technological affordances. In a recursive manner, these led to an expansion of the visual mind map as well (see time slices in Appendix 4). A few of our notes led to more data collection and additional interviews (particularly in the latter stages of the research that involved the digital forensics team). This added to our understanding and expanded the extracted affordances. Finally, the full list of affordances allowed us to refine the TIDM model further. A diagram of our grounded theory approach is shown in Appendix 5.

#	Interviews (I) & Observations (O)	Scope
1	(I) Two individuals from a large non-profit focused on Internet safety for children	Interviews on the general domain of online abuse and impact on children. (interviews conducted online)
2	(I) Two individuals from the Safeguarding Children Board of Local Council	Positions of interviewees were designated as “Internet Lead” and “Manager” of the Safeguarding Children Board of Council. General discussion
3	(I) Former Director of Intelligence at the National Crime Agency (NCA)	Strategic, technological and resource challenges in tackling online CSE & evolution of Phenomenon (two follow-up interviews on coordination for tackling online CSE)
4	(I) Detective Inspector X at Local Police Force 1	Policing Child Sexual Exploitation/Pursue/Investigations Follow-up interview on statistics for CSE
5	(I) Detective Chief Inspector Y at Local Police Force 1	Management challenges of CSE, evolution of investigations, indicators
6	(I) Detective Inspector Specialist, Command Cybercrime (CCU)	Combatting Online CSE, Policing, Investigations, Forensics, Imagery at Local Police Force 1 (CCU)
7	(O) 21 Participants –*Closed* (i.e. Private/Invited)	6-hour session [cyber-culture, online exploitation, online education, awareness] Training session on Online CSE in Local Council
8	(I) Police and Crime Commissioner (PCC)	Challenges faced when Tackling CSE at Local Council 2
9	(O) 11 Participants – Public Session on online CSE awareness (Local Council 2)	Police Training, Prison System, National Working Group on tackling CSE, Young Persons' Risk
10	(O) 12 Participants – Two *closed* sessions	Technologies and social networks related to online CSE and school liaison roles at Online Strategy Group of Safeguarding Children Board (Local Council 1)
11	(O) 20 Participants –*Closed* (i.e. Private/Invited) session on online CSE	Child safety in schools (Handling IT systems for schools and the deployment of a new filtering tool as well as e-safety training) in local Council 1
12	(I) Former Director of Intelligence (NCA)	Strategic issues around the deployment of information systems around online CSE and managing future challenges
13	(I) Detective Inspector (CCU)	Role of the Protection of Vulnerable People (PVP) command in online CSE and Information Systems being used
14	(I) Detective Inspector (Manager of CCU)	Managing online CSE work through different information systems (focusing on the TARGET and FILTER information systems)
15	(I) Civilian attaché to CCU (Triage Manager)	Use of information systems in handling and managing the *triage* process of online CSE related material (focusing on the INITIATE information system)
16	(I) Detective Inspector (Digital Forensics Manager-CCU)	Use of information systems in the digital forensics process of online CSE

Table 2: Primary Data Collection Sources and Scope

TECHNOLOGY & IMAGERY: TWO MAIN DRIVERS OF ONLINE CSE

Based on our primary and secondary data, we now focus on discussing our findings. Here we discuss imagery and technology for offenders, and then the role of children and parents. Then we present and analyse the different characteristics of our Technological & Imagery Dimensions Model.

Imagery and Technology in online CSE: Offenders

Offenders use technology and imagery in a number of different ways. They will either *manipulate* photographs by using image-editing software, *distribute* child pornography (e.g. through P2P networks, paedophile online groups, dark web), and/or *create* 1st generation images (i.e. original imagery). An additional element that we found to be critical in child exploitation online is that of *time.* Based on the FBI cases we analysed, months or even years might go into developing online trust to lure victims; this was also confirmed by interviewees #4 and #5. In one case, the offender was pursuing the victim for 2.5 years before sexualized imagery was divulged by the victim. Offenders also use imagery to gain the trust of victims and to mask their online identity. Between offenders, the exchange of imagery has evolved; based on our interviews with the police (#4, #5, #6) but also the observation sessions, offenders develop, build on, and adjust an online "esoteric language structure". An example was given by #6 who narrated an online discussion between paedophiles. One asked: "Have you got PTHC?" – and the other retorted "Sure". Then the police officer told us that this was "their code for Pre-Teen Hard Core" and it would often be seen split further in longer sentences to escape algorithmic detection

on a keyword-basis (e.g. "***P***articipate this coming ***T***uesday and don't forget to ***H***elp those less fortunate this ***C***hristmas"). Despite some efforts to issue warnings to users (e.g. if a user were to search on Google for 'child pornography' they would get a warning of being reported) and some encouraging results that paedophile searching online has dropped through traditional search engines, our interviews indicate (predominantly #2, #4, #6, #7) that this activity has been pushed to the dark web. There, it is much more difficult to follow (#6). Even an accidental discovery of a Virtual Machine (VM) from a confiscated laptop examined forensically by the CCU, led to a ten-month investigation that has not yet unravelled the dark-web activity of the offender who was receiving bitcoin payments for child pornography. Our interviewees suggested that it is mostly intelligence agencies that have the capacity to explore such activities, but without direct access, we could not verify the circumstances of the role of intelligence agencies in online CSE.

Imagery and Technology in online CSE: Children and Parents

Our data suggests that the way in which young users and parents use technology fuels the growth of online CSE. Since this is not their intention, we treat this here as a set of misperceived enabling affordances. Based on several interviewees and observation sessions (#2, #7, #9, #10), young users tend to ignore advice and/or misuse technology. The examples given to us included young people: i) violating terms and conditions of social networks routinely, ii) lying about their age to gain access, iii) creating online profiles despite age-appropriate notifications, iv) behaving irresponsibly online with an attitude that is shaped by the average age of their exposure to pornography (estimated at ten years old in the UK), v) displaying an apathy towards privacy online (reinforced by how parents behave online).

In this context, web-based relationships replace real relationships and increase the risks for children. According to #2, the act of children sharing naked photographs of themselves has been normalised so much in web-based relations that children refer to those as just “pictures”. Failing to realise the consequences of image distribution and data permanence online makes young users easier targets for serious criminals. Illustrating such young user attitudes and behaviour was a local council initiative that provided a custom-built “safe online networking platform” for students, which was abandoned since young users would “refuse to lock down their profiles and privacy settings” (based on both #2 and #1). Furthermore, as large circles of “friends” demonstrate popularity, discussions in observation session #7 corroborated that young users “purchase” online friends from online services that sell followers, likes, comments, etc. for Facebook, Instagram, and other social networks. As an example, $16 would buy 300 Facebook friends and get 100 likes, all delivered within 2-3 days. These are provided by “digital sweatshops”, with workers “befriending” users when an order comes in. Of course, young users who are desperate to grow their online following are easy prey for predators. As #6 suggested, children could be targeted based on their number of friends and their perceived popularity. The data suggested that more popular children, measured by a higher number of online friends, were targeted more. Another accelerating factor is how parents use technology. Parents generally lack “e-parenting” skills and (over)share imagery of their children across multiple social networks. This is the raw material that is exploited further. Based on #3, while parents cannot usually contemplate why someone would download images of their children, the answer often remains: “because they’re available” (#3).

From our interviews with #1, #2 and #8 as well as observation sessions #9, #10, we find several interconnected elements whereby oversharing parents recursively fuel online CSE: i) legitimate photos that were uploaded by parents are downloaded, sexualized and re-circulated as part of online pornography, ii) as children cannot give consent, parents are effectively violating the privacy of their children by posting online and they further iii) cultivate the apathy of children towards online privacy (desensitization), which makes children more vulnerable to future victimization, iv) location-sensitive information can be part of a photograph's metadata and children can be targeted for contact sex offences, v) phenomena like cyber-bullying often use imagery from parent profiles, vi) the co-mingling of fake pornographic imagery (as an unintended consequence of parental posting) with 1st generation imagery (i.e. original imagery of novel cases) and 2nd generation imagery (i.e. imagery re-circulating from previous cases) creates detection challenges for cybercrime authorities.

STAGES OF TECHNOLOGICAL USE IN ONLINE CSE

Based on our grounded theory approach, we identify four key stages that underpin the centrality of imagery in relation to technological use (see Figure 1). These stages are: initiation of contact, trust development, online extortion and trafficking. They revolve around technology and imagery, two dimensions that are structurally coupled. Through the use of imagery, technology affords online CSE by supporting the goal-oriented action of offenders.

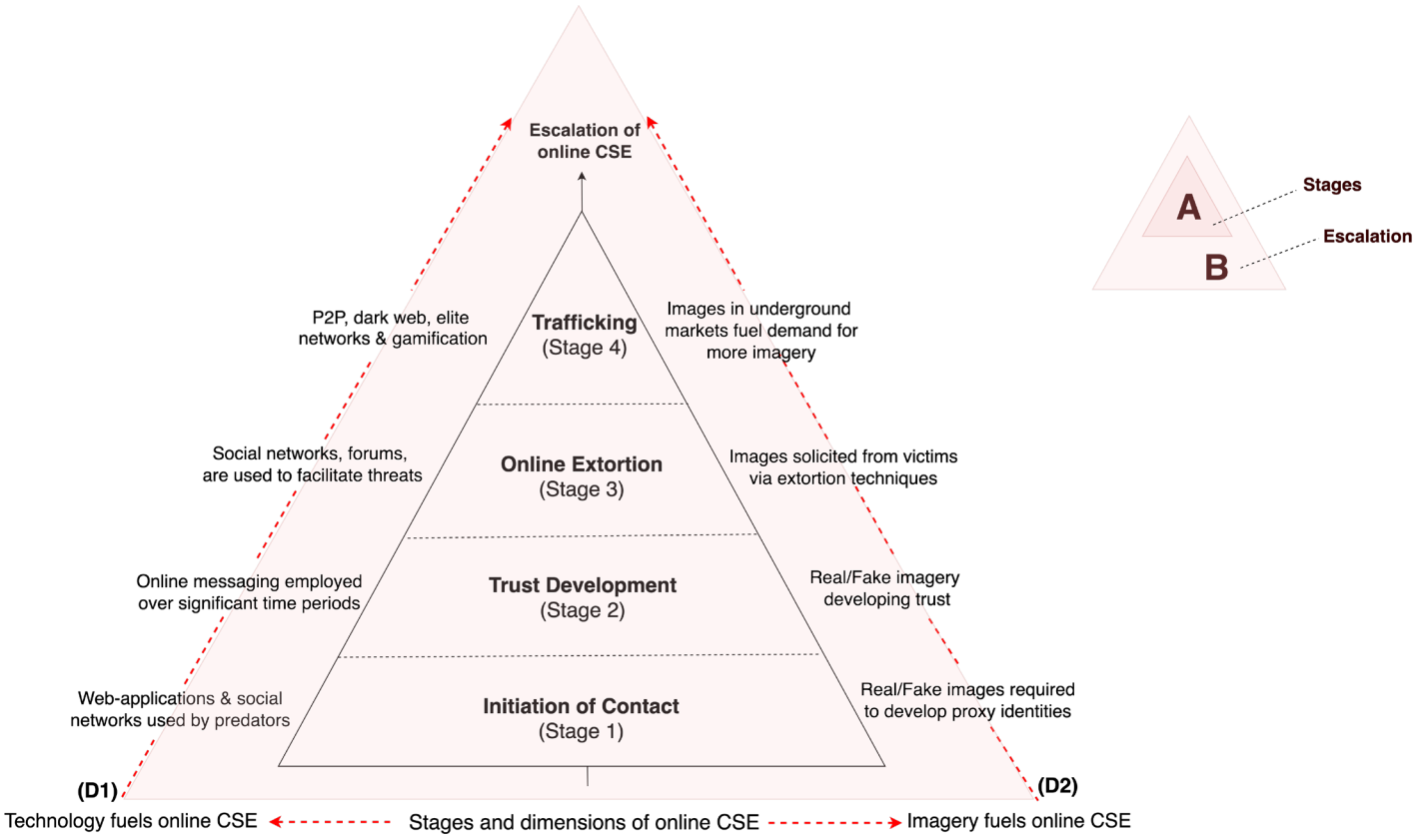


Figure 1: The preliminary Technology & Imagery Dimensions Model (TIDM) of online CSE (depicting only the offenders' side)

Stage 1: Initiation of Contact

At this stage, offenders use different social networks, web-applications and platforms with a goal to *initiate contact* with potential victims (dimension 1). To support that goal, offenders require a proxy virtual identity to create distance from their real identity (cybercriminals call this 'taking care of their own operational security' based on #3). In turn, as shown in dimension 2, offenders require real/fake images to convince their victims of their proxy identity and conduct digital deception. As the goal is to lure those children to produce authentic nude photos, this creates a recursivity that fuels the growth of the phenomenon. The reverse is

also possible while rarer: children seek out random connections themselves and volunteer nude imagery. As mentioned by #2: “remember when our parents used to say don't speak to strangers? Now children seek out to speak to strangers all the time through such (web) applications”. Meanwhile, the exploitation of platforms by tech-savvy paedophiles has escalated. There is evidence of bots being programmed to lure children. They initiate contact by posting an appealing message, sign-off, and let an offender on another platform take over. Based on #5, “in prison it is known that paedophiles buy/sell addresses of vulnerable children in exchange for cigarettes, but in the online world, they cooperate on many different levels”.

Stage 2: Trust Development

In this stage, the goal-oriented action of offenders is to gain the trust of their victims, often over long periods of time (dimension 1). In one of the FBI cases, a twelve-year old had received 1200 messages over a two-year period. While imagery becomes critical in trust development (dimension 2), the techniques being used by offenders to gain trust vary, with location-tagging perceived to be more dangerous as victims can be targeted for more serious, in-person crimes. An example from the FBI cases is the “new kid on the block” technique (dimension 1), where offenders will pretend to be young children themselves that have just moved into the area. The act of “checking in” at a location nearby creates a false sense of trust. The critical role of how digital imagery affects this stage must be highlighted. For offenders to fulfil their goal and make potential victims feel comfortable, they will proactively offer nude images of their ‘online persona’ (dimension 2). While real images might be used as well, the sexualization of harvested images of children seems to be more dominant at this stage, with use

of face-swap software and AI-based deepfakes (Kietzmann et al., 2020), allowing offenders to create photorealistic imagery easily (dimension 1). Overlaying a child's naked body over multiple faces allows offenders to create multiple proxy-identities for the parallel exploitation of different victims. The over-abundance of children photos (dimension 2) makes this stage much easier for the offenders.

Stage 3: Online Extortion & Threatening Behaviour

Once victims are convinced to expose nude photographs of themselves, offenders engage in threatening behaviour and online extortion. Offenders may start posting "soft" material that exposes the victim on public websites or social networks (dimension 1), divulge intimate conversations, even threaten to kill the victims or kill their family members if their demands are not met. According to #1, this "constitutes a state of suspended humiliation or anxiety" that is extremely difficult for a young person to cope with. Victims may remain "compliant" for some time before they ask for help. The outcome is a highly disproportional relationship between number of victims and explicit images produced (dimension 2). In one example from the FBI cases, a 12-year old girl, under the stage of online extortion, uploaded 660 sexually explicit images of herself to a cloud-based storage account controlled by a 25-year old perpetrator before asking for help. In some cases, help is never sought. For offenders, the main goal is to maintain a continuous supply of explicit imagery (dimension 2). Based on our interviews, this pattern is broken if the offender seeks to commit more serious sex crimes, including kidnapping, murder, rape, child trafficking, and organ removal for the illegal transplants market.

Stage 4: Trafficking

In this stage, offenders are enabled by P2P networks, the dark web, proprietary forums, and their goal-orientation is to traffic child pornography (dimension 2). In addition to the secret groups that offenders use to exchange illegal images through otherwise legitimate social networks, we were also told of the existence of "elite child-pornographic networks" (dimension 1) where online access is 'bought'. The centrality of imagery comes into focus here as it is the pornographic images of children themselves that are being used as a virtual currency. Based on our interviews (#3, #4), the threshold of buying-in access varies, though we were told of one example of a network requiring a minimum of 2,000 images as an ante. The use of illicit child imagery as tokens in such underground economies is what prompts aspiring 'elite' paedophiles to make up for the difference in images that they do not hold in their possession.

Thus, these individuals engage in the practice of harvesting photographs of children from social networks and other web-based sources, and manipulating them so that they appear pornographic. Alteration of imagery serves the double purpose of establishing fake online identities (at stage 1) and gaining token-based access to elite networks for trafficking (stage 4). Monetization is also a factor here. As #6 mentioned, we're entering a "space where requesting payments in Bitcoins or creating new online-CSE-related digital currencies like paedopoints might become the future norm". This reinforces Westlake's description of criminal careers in cyberspace. Based on the interview with #6, the case of Richard Huckle was mentioned as an example at this stage. Huckle, having abused more than 200 children himself, had thousands of images and videos depicting child abuse in his possession (mostly 1st generation imagery). The complexity of this one case, the associated digital forensics analyses and the investigation took almost a year before Huckle could be arrested. To make matters worse, Huckle had used

technology to develop an online community and to award ‘paedopoints’ (a virtual token) based on other offenders sharing evidence of their successful exploitation of children (dimension 1). If offenders were not advancing on Huckle’s leaderboard, they were banned from the forum. Huckle had ‘gamified’ online CSE and he was using child imagery as a tradable currency (dimension 2) amongst a small criminal community of trust. He had even drawn plans to monetise them for Bitcoins just before his arrest at Heathrow Airport. Huckle was convicted in 2016 for 71 counts of serious sexual assaults against children. In that context, cryptocurrencies, the dark web, the over-abundance of photographs of children that can be manipulated and unsafe online behaviours across all social networking platforms, fuel the dynamics of online CSE (dimension 1). This creates a challenging context for cybercrime police at the CCU. The next section discusses these challenges before relating them onto the TIDM model.

LAW ENFORCEMENT INFORMATION SYSTEMS USED TO FIGHT ONLINE CSE

In exploring online CSE in the organisational context of the Cyber Crime Unit (CCU), it became evident that a variety of Information Systems were used to counter the phenomenon. We differentiate between peripheral IS that can be used in online CSE investigations and core IS that are essential. We have anonymized the names of several IS where necessary.

Peripheral Law Enforcement IS used in the fight against online CSE

As an example of peripheral IS for online CSE, two information systems used by the Police are Watson and HOLMES 2. While we were told that the latter would only overlap with online CSE if a murder was recorded as well, the former system (Watson) was an analytical tool

that would link intelligence with suspects, criminal groups, and locations. However, based on #6 who has been investigating cases of online CSE for nearly a decade, the collection of intelligence for suspects is scattered across different IS. Combining intelligence from many different sources (schools, health & social services, public, police supporting services[2]) to a fuller picture of a suspect is time-consuming and challenging. While there are some interoperable systems, a detective looking to develop a comprehensive profile of a suspect would need to combine intelligence and access different systems. To counter that fragmentation, #4 mentioned that he was "forced to develop" an Excel spreadsheet on his own so that he could "register different bits and pieces for CSE suspects" and "provide end-of-year CSE statistics to his superiors". Recognising this, #5 said that the Association of Chief Police Officers' strategy for ICTs recognised "that the police service in England and Wales can no longer afford to treat ICT as isolated programmes of work developed and operated independently by separate organisations".

A more extreme variant of this problem was discussed by #13 who mentioned that between two critical teams for online CSE[3], there was no meaningful channel of communication. For instance, based on #13, one team could be investigating a possible child abuse case but lack skills around technology that would enable it to identify online CSE as an additional criminal dimension. Based on an observation session (#10), this was identified as a broader issue of organisational disconnect. As mentioned by #13, there are "different command areas" that are

[2] An example of this within UK Police is the PVP department for the *Protection of Vulnerable People* that may have information about children that might need to be safeguarded and where online CSE could be a consideration.

[3] One being the Internet Sex Offenders team and the other being the PVP (Protection of Vulnerable People) team

"not joined up" and this raises a broader child safeguarding issue. While the CCU is at the core of handling the ongoing cyber-risk, safeguarding children transcends many different departments within the police and also involves external stakeholders. For instance, in observation session #11, the deployment of filtering tools was discussed for schools. The head of IT services for all schools in the local community explained how a new software "picked up keywords that might indicate specific vulnerabilities" related to online CSE. She mentioned that some online searches of children at schools were "bringing up some horrendous hits – some really severe hits". While this school filtering tool has been "working for about a month at an experimental level at only seven schools", it became clear that the manual review of the volume of red flags is beyond the capability of any school. A full-scale deployment would require a clear policy of how cases should be prioritised. Despite a clear, and agreed-upon need to deal with online CSE in a risk-based approach, the sporadic implementation of many different and disconnected technologies makes such initiatives increasingly difficult.

Core Law Enforcement IS used in the fight against online CSE

Of course, technology is not only used by those who break the law, but also by those trying to uphold it and pursue offenders. Our study revealed a combination of different, at times overlapping core law enforcement IS. These include network monitoring systems, data filtering systems, systems developed to triage and prioritize the severity of images and offenders, risk-assessment tools, and specialist digital forensics. In the following subsections, we discuss these systems and how cybercrime officers are enabled and constrained by these in their goal to fight online CSE.

Law Enforcement IS 1: Network Monitoring

While the streamlining of communications is challenging in the context of online CSE, there remain core IS that enable officers to identify 1st generation imagery and pursue offenders who have a higher probability of being contact sex offenders (1st generation imagery is associated with potential "ongoing victims"). In this context, one of the core IS used to tackle online CSE is the INFOTRACK system (our alias) that is handled at the national level and administered by UK law enforcement[4]. INFOTRACK monitors peer-to-peer networks for files exchanges. It identifies and collects imagery to be investigated further. Part of this mechanism includes filtering out those images that are 2nd generation (that have been recirculated). This initial determination is achieved by the use of a database called CAID (Child Abuse Imagery Database) that became fully operational in December 2014. This database contains hashes of known child imagery in circulation. Thus, when an image is collected by a P2P network, it is hashed by an algorithm. When the hash is identical to an entry in the CAID database, this image will be recognised as a 2nd generation image that has been circulated/evaluated before. While the trafficking of 2nd generation images remains an offence, it is considered as low-risk for purely follow-up investigatory classification purposes. While image alteration (even by a single pixel) would result into a different hash altogether, the application of specialist image recognition software would attempt to (re)classify these photos further based on previous ones in circulation. One such example is PhotoDNA, developed and provided free-of-charge by Microsoft.

[4] More specifically, by the National Crime Agency where the Child for Exploitation and Online Protection Centre is based (known also as CEOP)

The deployment of INFOTRACK along with the complementary use of image recognition has brought with it additional demands in how technology can be used. An example is the "additional needs for police officers in the field who are now photographing empty rooms of offenders" (#16). The physical characteristics of known rooms in which offenses have happened might be linked (through image-recognition) to previously trafficked images and cases of exploitation. Thus, if the offender used the same physical space to conduct/record their activities, previously unresolved cases of victims and corresponding imagery could be associated with that offender. However, all of the 1st generation images have to be reviewed, one by one, by police officers who evaluate the seriousness of the depicted abuse and categorise 1st generation imagery at the level of local police forces in the UK. With the fear of stating the obvious, this is probably the most stressful user-group of any information system as they have to "view gruesome images of child abuse as their day-to-day job" (#16) and then feed their results back to the database (in case the same image recirculates in the future). While some sporadic technical glitches have hampered the work of police officers as the "connection might have a problem" or the "speed of processing varies", the users generally view the INFOTRACK system favourably. It has enabled them to reduce the processing time and largely lifted the burden of verifying 2nd generation imagery that remains the "vast majority and accounts for probably more than 90% of the imagery trafficked" (#14). Through INFOTRACK, users conduct computer-assisted/manual 1st generation imagery classification, risk scoring, and offender profiling.

Additional constraints are that INFOTRACK "is not a permanently-on connection and it focuses on P2P networks only" (#13). The rest of the leads are referrals from technology companies. As #14 mentions, the "main ones that we have at the moment come from KikMe,

Facebook and Dropbox, but we get referrals from many". This was the subject of a more general discussion with several interviewees who felt that technology companies at large are not doing enough to tackle the phenomenon. However, some relationships between the Police and Internet Service Providers (ISPs), as well as different technology companies, are at times challenging. First, although some national police authorities will act to develop software for reporting child online abuse, their operations will not be supported by technology companies. For example, the UK's national centre for Child Exploitation and Online Protection (CEOP) had developed an online abuse button that could be integrated across different social networks and websites. However, we were told that Facebook declined to integrate it (#2, #3) and has other internal measures and lines for users reporting abuse, which can then be forwarded to the Police (#4). Also, a number of hashes from the CAID database are fed back into technology companies so that the images can be removed. However, without research access to Facebook itself (or other social networks), we cannot ascertain the enabling/constraining affordances their analysts would experience. Second, collaboration with ISPs is not always straightforward and they exhibit variable degrees of cooperation. Based on #6, strengthening these collaborations and establishing better processes for data exchanges need to be explored further. For instance, hardware black-box filtering at the ISP level is one countermeasure that can be explored to enable monitoring, though its application would (and should) be constrained by strict privacy safeguards as misappropriation and surveillance would need to be factored into any decision-making.

This reflection of further countermeasures extends to the police as well. Based on different interviewees (#3, #7, #12, #18), it is evident that the police's use of INFOTRACK is *reactive* although *proactive* techniques that "sniff out *potential* offenders" (#16) would be more

effective. For instance, police officers assume ghost virtual identities online when they pretend to be children themselves and chat online with potential offenders. The use of proxy identities online then is a shared affordance between offenders/police as behavioural mirroring through technological appropriation creates the potential to unearth offenders. We were also told of "online vigilantes that do the same thing and then report to police" (#6), though these were limited occurrences.

Law Enforcement IS 2: Data Filtering

Since the challenges and the dynamic language structures that offenders use to "find themselves online" (#12) escape detection thus far, current developments of countermeasures will involve real-time proactive filtering. As the emphasis is changing, we were informed of the experimental deployment of the HARVEST (our alias) information system. This was a real-time filtering solution that was tuned to "listen to social media by fixed search keywords that were set by the police" (#16). The goal was to deliver intelligence on online CSE and develop an automated identification mechanism for high-risk classifiers (e.g. gender). While a sample profile was not disclosed, the organisational consequences from the use of the HARVEST system were discussed. In the trial, the "overwhelming majority (of suspects) was meaningless" (#6) and eventually the police had to "shut the system down completely" as the examination of false positives consumed valuable resources.

Based on nearly all interviewees, the top challenge across the use of technology in online CSE can be summarized as a "coping with the data deluge" problem. While initiatives like the database of hashed 2nd generation imagery (CAID) have helped considerably and allowed the "force to focus on the quick identification of victims", the "massive data dumps from across the

world" (#3) are daunting and pose significant challenges for any police force. Within a timespan of a few years, the phenomenon has demanded increasing resources. In fact, at a moment in time when UK forces are experiencing budget reductions and crime has seen a 10% increase throughout the country, there are two growth areas that have become critical in policing. These are (according to #3) cybercrime and online CSE. Whereas back in 2005 there were about 10-20,000 images related to child pornography and abuse, we were given an estimate of 26 million images for the UK alone from #2. This rough estimation and official reports of images "in the millions" (CEOP 2016) shows the scale of the challenge. For example, as we were told by #3, in one of the massive streams of data, in just one day, the UK had received 100,000 distinct IP addresses and related images from the US-based National Center for Missing and Exploited Children. While this was a "burst of activity" that did not represent average daily operations, it served to illustrate how swiftly these challenges can escalate. The IP addresses were passed onto the UK command and the images were compared with hashed versions of 2nd generation images. Based on approximate geolocation, the IPs would be forwarded to the 45 police forces in the UK where the abuse-images would be assessed, ranked, and prioritized and suspects would be evaluated. The challenges in this process are plenty.

As the CCU says (based on #6), the unit receives IP addresses and some basic information about the indecent imagery that has been detected. In that context, the CCU submits further requests with ISPs in order to identify individuals behind such IP addresses and pursue their investigation. Occasionally, the simplest of technical issues would create a butterfly-effect down the chain of investigations. For instance, one of the issues mentioned by #12 and #13 was that sometimes there's an issue with wrong IP addresses being recorded as part of the monitoring

mechanism. If a router refreshes its IP address (e.g. restarts), the old IP address that was linked to illegal trafficking could be assigned to someone else and the "intelligence analyst assigned to the case may take it as far as a warrant…someone may get a knock on the door and have his equipment seized and it might take some time to analyse their devices before we realise we've got the wrong person…on another occasion we ended up in an empty building due to a mix-up with the physical address… if there are many people in a house then we have to check for the GUIDs (Globally Unique Identifiers)". While the aforementioned examples are exceptions, there is a general acknowledgment that there are "several issues with IP resolution at a national level" (#15). Most of the time, the challenge is the sheer volume of imagery to be examined. Once INFOTRACK helps separate 1st/2nd generation imagery, the question becomes how the 1st generation images will be analysed by cybercrime police and how offenders will be prioritised. Several IS are used throughout these phases. In this context, we must remember that offender-driven demand for imagery as delineated in our TIDM model (setting up proxy identities, establishing trust between offenders/victims, etc), all fuel the data deluge around this problem.

Law Enforcement IS 3: Online CSE triage

Precisely due to the volume of data and images to be handled, there is a separate data *triage* process that aims to prioritize cases on two fronts: i) the severity of images, ii) the profile of the offender. In the context of the first, *triage* is conducted using the INITIATE information system (our alias). Once a warrant has been executed, the confiscated devices are brought to the CCU for the triage process; this is not a full forensic examination that would stand up in court (that would be handled by the forensics department) but another layer of prioritization. According to the manager of the triage department, the team's role works "much like a hospital

triage process and tries to get the critical cases quickly to the forensics department so that the offender can be pursued in court…however, there is a backlog and a massive queue that could take months to clear out" (#15). One of the key challenges emerging from the evolution of computer storage is that the triage process has changed substantially over the past years. As mentioned by #16, some years ago we would "confiscate a desktop disk, possibly a laptop… nowadays police officers come back from a suspect's house with desktop hard drives, laptops, several SD memory cards, plenty of USB sticks, external hard drives, mobile phones, etc". On one case alone, the Police had confiscated a total of "17 devices" and this is something that "complicates both the triage process and the full forensic examination and makes it more time consuming" (#16). Referring to a single case within the CCU, "it was impossible to look at the 1.5 million images we found across his devices; if we were to do that, we would increase the risk of (mis)handling other cases" (#15). The balance that needs to be struck in managing cases/volume is challenging due to technological variety and new demands posed by new developments (e.g. cloud storage, the TOR browser that gives access to the dark web).

Despite the variety of technological artefacts used in tackling online CSE, the triage process is relying only on the INITIATE software. This is a shared collaborative tool amongst a small team of officers. Once the devices are docked and the content is mirrored for the examination, data extraction begins. This "includes deleted photographs/videos and communications data while the whole process is documented based on national guidelines" (#15). Then, by using the INITIATE software, users will scroll through the extracted material in the user-interface of the software and manually categorise any material on a scale of 1 to 10 based on severity. They will then create a report for the digital forensics department for a full

examination. The underlying basis of how the software will scan for extracted material and designated file-types can be customised and "users do tend to create their own profiles where a lot of filters that can be (de)selected… even though there is always the option of asking the software to find as much as possible in one go or use one of the eight different built-in default search profiles" (#15). As an example, a detailed search profile[5] will collect allocated, embedded, deleted pictures and videos, search for common keywords related to online CSE, search for known hash values, collect received files from various applications (e.g. Skype) and other media cache folders, office documents, registry files, search for anti-forensic applications, collect user desktop shortcuts, and so on. Processing times will vary depending on the filtering mechanism used but one indication given was that 500Gb would take a full day for processing. On some occasions, a scan could be running for two weeks and produce terabytes as a report. As considerable time is required to scan the devices confiscated, "users will often stop the scan if they think they've seen enough" to secure prosecution, though "90% of the time we let scans run to the end". Of course, the danger for the remaining 10% is that the analysis might be missing 1st generation images. Such a near miss was the attempted rape of a 2-year old by his father when the related image was extracted at the very end of the scan.

The adjustments on the sensitivity of the profiles for filtering is an additional concern. The INITIATE software allows for several different options, including ranges, pattern modifiers, quantifiers, sample pre-fixed patterns by the software company. The very act of the necessary ad-hoc selection by triage users at CCU leads to the risk that the technological profiling mechanisms

[5] Known as a full IPOC search (Indecent Pictures of Children)

through which content is analysed and suspects are identified are not appropriate. In other words, what gets flagged and evaluated is contingent on whether the related filter(s) that will yield the result is selected or deselected. Reflecting on the technological contingencies, software-use, profiling methods used and the nature of the phenomenon, the following six key concerns emerged from the analysis of our interviews (mostly #15 and #16). First, the really technically skilled offenders may be escaping detection as any custom filters that would detect their behaviour might not be applied. Second, capacity for staff members that can actually conduct such triage scans and use the INITIATE software is limited and must be increased but lack of practice and training were identified as inhibitors. Third, the backlog of confiscated devices to be triaged has (periodically) increased to nine months. This is often quickly ameliorated by outsourcing some of the workload, though the financial sustainability of outsourcing such work is problematic. Fourth, cloud-based storage and related applications complicate the process time-wise as a preservation order is required for limiting the suspect's access to the cloud before the data can be mirrored and analysed. Fifth, as mentioned previously, users who are working with such imagery undergo an annual mental health evaluation so all users of INITIATE would fall into that category. However, based on #14, it would be much more interesting and considerate if user-stress evaluation was built into the use of such triage software on an ongoing basis. This could identify users under stress based on behavioural patterns of software interaction. Sixth, while INITIATE triages data captured from confiscated devices, there is no capacity to examine anything related to the dark-web and such investigations are within the remit of national-level agencies (e.g. in the intelligence community).

Law Enforcement IS 4: Risk Assessment & Prioritization

In parallel to the use of all the above systems, another tool is used that we anonymise as TARGET. This software is being used as a standalone tool in order to evaluate the potential risk that an offender might be a *contact sex offender* by conducting behavioural psychological profiling. As #13 mentioned: "the filtering mechanism is conducted by applying a classification tool that helps us prioritise our workload". Even though we have received a copy of the TARGET manual from the police, we have been asked not to disclose how this tool works in detail as the material is classified as 'Official Sensitive'. Thus, we restrict our description to broad functions. Through a series of questions that the user (i.e. the police analyst at the CCU) is asked by the TARGET system, a high/medium/low risk is assigned to each offender. This is specific to whether the offender could be a contact offender. For example, individuals who have 'easy access to children', for instance by working in a school, receive a relatively high-risk weight for 'access' from a preselected list. Clearly, high risk scores receive overall priority. However, building the intelligence profile for a suspect is time consuming and takes about one week (or two to three days if there are additional concerns that would elevate the prioritization). According to both #13, #14, managing this "ongoing risk" by using technology in various forms (e.g. different software) is the single biggest challenge, particularly since the victim could be anywhere in the world and cross-border communication would transcend several different systems and scattered intelligence about offenders. Perhaps a surprising element in the context of using the TARGET system is its complete disconnect from the assessment of imagery. In terms of the future development of information systems in tackling online CSE, refining the risk-scoring for potential contact sex offences and providing simultaneous risk indicators through imagery for profiling and prioritising suspects is highly desirable. At the moment, the TARGET

system “doesn’t care if the suspect has downloaded one illegal image or 100,000 images – it’s based on psychological profiling alone” (#15). This provides counterintuitive results as the person who may have downloaded one image may be posing a higher risk. Again, the issue of interoperability/intelligence-sharing between different IS comes to the surface.

Law Enforcement IS 5: Digital Forensics

The “last stop” of the process is the forensics department of the CCU. Its manager echoed the concerns above while adding additional issues. “Resourcing against increasing demand” remains a substantial challenge. As #16 mentioned, “a member of staff would undergo 12-18 months of specialist training to use the (information) systems we have here... and then of course, there is a more general technical knowledge issue and training of police officers in the field. For example, they may file a report on a confiscated mobile phone, and the report asks them to fill out what an IMEI is and they wouldn’t know that”. A “basic level of being comfortable with IT” was considered essential. Police officers, through no fault of their own, present a risk into what intelligence is fed into different systems (e.g. incomplete or mistaken data entries).

Within the forensics team, several computer-based systems are being used; this variety contributes to the training time required. Limited staff resources mean that “people are doing things they shouldn’t be doing” (#16). For instance, mobile phone extraction software users are overburdened so their cases are allocated to other officers that are less familiar with the software. Also, while a few primary forensic software tools are used to examine confiscated devices and the same image categorisation tools that follow up from the triage process in order to classify images based on sentencing guidelines (A- extreme imagery, B-medium, C-least extreme), the biggest demand for hardware/software is for mobile phones. In that context, the forensics team

"use two specialist applications but there's an increasing need for mobile docking stations dedicated to mobile phone analysis" (#16). The kiosks that analyse mobile phones are in top demand; and even though the forensics team examines all seized exhibits, determining the priorities for each case is not always straightforward. Based on an estimate given to us, 42% of the examined mobile phones led to drug-related intelligence and "removing a lot of that volume out of the office" is not always straightforward. There is an increasing need for faster hardware/software configurations that will triage mobile phones and identify low-level crime, re-direct it, and allow the team to focus on online CSE.

Perhaps one of the best examples where a specialist information system will pose demands for both officers in the field and for the forensics team is the REVERSE system. In tackling online CSE, although encryption safeguards legitimate transacting, "encryption is an obstacle" based on #16. When pin-locked devices are brought into the forensics team and devices are password-protected, the team tries to get around the security measures by hacking into the devices so that the content can be evaluated. The REVERSE software aims to address this gap: it also takes *physical* evidence that are collected by police officers in the field, including among other evidence types, letters, bills, and anything else that police officers can consider as important. It then combines them with other pieces of information collected electronically and generates a list of passwords from such bits of intelligence to gain access to the device(s). If this stage fails and access to the devices is not secured by the forensics team, the CCU resorts to a

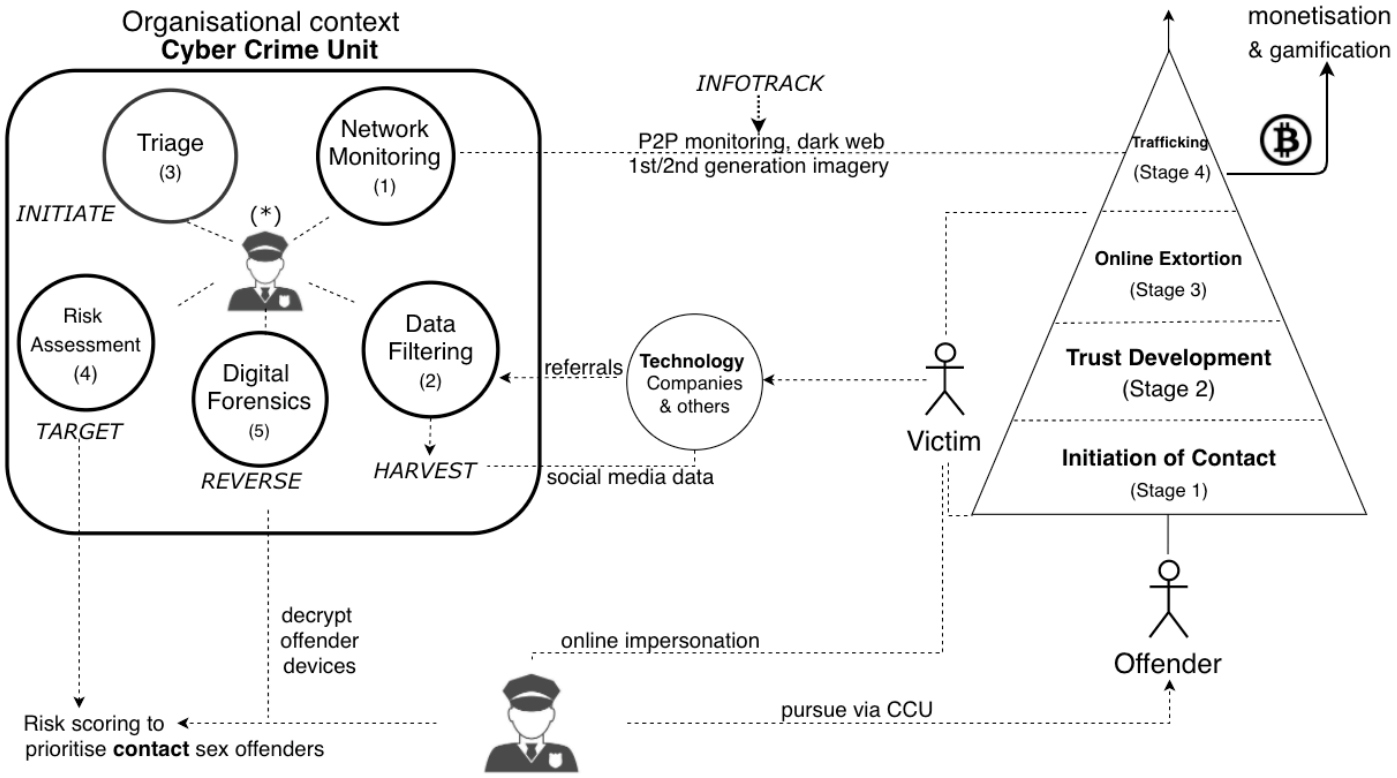
legal process[6] which demands that suspects supply their passwords. Failure to do so renders them liable for prosecution but this process is a "costly legal resort. If decryption fails, [prosecution] cannot be instigated without national approval and realistically very few people get convicted" (#16). Thus, from the point of view of the forensics team, encryption is a significant constraint.

The specialist use of such IS has recently led the UK government to re-classify all digital forensic departments as laboratories, prompting all to achieve international accreditation[7]. This strengthens the legal admissibility and evidential weight of electronically-harvested, analysed, and categorised digital information. It also safeguards the processes used throughout online CSE investigations and minimises further any risks for third-parties "planting incriminating information like in the case of a male suspect who was innocent and his ex-wife had planted child pornographic imagery on his computer to gain custody of their children" (#13). Working towards accreditation is creating "several new organisational demands that will require a persistent effort… the simplest one being the recruitment of specialist personnel to guide us through this process and a quality manager", as well as "changing the processes to fit the standard" (#16). However, the subtle issue of how different information systems construct the prioritization and identification of suspects remains. Put differently, technology-use in online CSE constructs the pathways through which suspicion is identified in complex ways. We would prompt other IS scholars to explore the variable technological construction of online CSE at the

[6] In the UK, this would be invoking Process Section 49 of the RIPA code (Regulation of Investigatory Powers Act)

[7] ISO 17025

level of suspicion. How algorithms and technology-use prioritize and allow certain suspects to emerge, while others are either deprioritised or dismissed, is of pivotal interest. The development of algorithmic accountability in such contexts remains critical. Ultimately, reducing the complexity of online CSE through IS-use is reflected across all stages. When it comes to dealing with the prosecution of online CSE, "a lot of forensic labs have set their criteria to 250 Class A imagery while over 50 Class A designations would stand up in court" (#16). However, the use of different IS and filtering restrictions creates a forceful reduction of complexity and creates additional risks. Based on #15, on one such example, "the totality of devices indexed had 1.4 million images to search through but the software got only 0.01% because of filtering restrictions…on occasion, we're running a big risk for unknowns". The alternative of a manual analysis is unrealistic given the volume to be examined. While diagrams simplify and reduce the content, the framework in Figure 2 summarizes some of the core aspects discussed above and brings together the preliminary TIDM model with the organisational context.



(*): Due to the nature of work and IS use, specialist training of users is required in an environment where user stress is amplified. A skills shortage is also identified, particularly in some areas of digital forensics
(1):Network monitoring is largely oriented to P2P and is not a permanently on connection. Dark web traffic and investigations exhibit complexity and are usually handled at national level by intelligence.
(2):Data from various different sources are used at the CCU; these are either 1st generation or 2nd generation imagery from INFOTRACK, referrals from tech companies, intelligence, social media data, etc
(3): The triage process aims to prioritize the severity of the images and the the profile of the offender so INITIATE is being used to categorise the severity of the mterial before being passed onto the forensics team
(4):A variety of different software applications are being used within the CCU in order to tackle online CSE. These are described separately across the preceding sections. TARGET risk scores offenders
(5):Hardware demands revolve around storage in the forensic team and docking stations for mobile phones. Systems like REVERSE assist in the decryption of offender devices.

Figure 2: IS in online CSE

Figure 2 above connects the main staging (stages 1-4) of the TIDM with the organisational context in the CCU and the different IS used to tackle the phenomenon. First, on the right-hand side of the diagram, we notice that stages 1-3 demand the participation of both victims (children and parents) and offenders. However, stage 4 is somewhat distinct in that it occurs through P2P networks, elite paedophile communities and dark web markets. Thus, as an activity, stage 4 can occur independently but is also fuelled by the continuous stream of activities that offenders initiate in order to lure more victims. Whereas we have seen the connections of

attempting to monitor trafficking through INFOTRACK, the constrain remains that this is not a permanently on connection. Real-time monitoring and increasing ISP collaboration in this context are very important but touch upon the sensitive debate of privacy vs security (Etzioni, 2015). Spotting 1st generation imagery quickly so that high-risk abuse and 'live cases' can be investigated, remains very challenging due to the volume of data, lack of resources, and a diffusion of intelligence. The variety of IS being used, often for complementary tasks, leads to fragmentation while hardware demands increase (e.g. mobile docking stations, decryption).

Furthermore, in the context of stages 1-3, the CCU relies on technology companies to report suspicious activity. Based on #3, #6, a common concern is that social networking and other technology companies are not doing enough to suppress the phenomenon. With information systems like HARVEST failing to capture real suspicions and the only other viable option for luring offenders being the conduct of online impersonation of children by cybercrime officers, we need to rethink the relationship between technology companies and cybercrime police in the context of online CSE. Some (#3, #14) argue for direct unlimited access of select cybercrime police to social media platforms but this is likely to meet resistance. Similarly, hardware black-box ISP filtering is one countermeasure that can be explored for stage 4 but this raises similar concerns on the propagation of a surveillance state, exploitation of access for other reasons and privacy violations. A combined exploration of this field alongside Privacy Enhancing Technologies (PETs) could lead to significant privacy-friendly monitoring innovations (Heurix *et al.*, 2015).

While the challenges presented across stages 1-4 are escalating, the organisational barriers at the CCU raise further difficulties in preventing and detecting online CSE. Separate

command areas between critical teams should work more closely together. Also, intelligence can be found across several stakeholders that are often outside the CCU that is handling the ongoing cyber-risk. While the core utilities of IS can be recognised to serve: a) the *timely* identification of 1st generation imagery, and, b) the identification and risk scoring of offenders who have a higher probability of being contact sex offenders, the two are not really linked. Furthermore, training staff for online CSE is complex and requires serious investment. Specialist knowledge (e.g. at the forensic level) is demanding but there is also an increasing need to educate field officers.

Overall, the technology-based prioritization of online CSE cases is complex. The role that technology companies play, as well as that of ISPs and many other stakeholders that can be involved in deploying online CSE countermeasures through specialist information systems is still emerging. As such, it is worthy of exploration from IS scholars. Most of the emphasis on countermeasures appears to be on how stage 4 (Trafficking) is handled through INFOTRACK while the application of filtering across different levels raises an additional issue: how the related IS are used and integrated, end up 'determining' who is forwarded for prosecution and who is considered as a suspect. This 'determination' is far from causal taken the variety of filtering options being used. Different approaches when managing online CSE investigations run risks for missing victims or flagging suspects in an inconsistent manner. Sadly, the online behaviour of both parents and children contributes unwittingly to the volume of child imagery as these are harvested and distorted from offenders and become comingled with 1st generation imagery. The multidimensionality of technological interferences and the challenges faced in online CSE, make the dynamic between technology and online CSE critical to explore, model, and reflect on. Below, we present the affordances of technology in online CSE (Table 3). We need to remember

here that artefacts can have both enabling and constraining expressions which are relational for different user groups; our emphasis remains on the relationality between *enabling affordances for offenders* (so that we can understand how their use of technology allows them to fulfil their goal to lure children) and the *enabling affordances* for the CCU (allowing cybercrime police to tackle the phenomenon). Each user group would have constraints: IS research should be conducted with a view to increase the constraints for offenders and decrease the constraints for cybercrime police. Our combined research into the stages of the phenomenon and the organisational context allows us to depict: a) how the escalation of the phenomenon occurs (from the perspective of offenders and how they use certain artefacts, features, images to achieve their goals) and, b) how the de-escalation of the phenomenon is attempted by cybercrime police. We accept the (unavoidable) limitation that there is a much greater number of affordances that can be captured and more research needs to occur within IS so that we can understand this phenomenon better. For example, technology companies like Facebook could be deploying their own technology artefacts, features of which would enable them to de-escalate the phenomenon but without access to Facebook as a research setting we cannot include these. Where an affordance can be considered as a *shared, collective, or misperceived* affordance based on our discussion in affordances, we indicate that in Table 3 below.

Affordances	**Technology Artefact(s) involved**	**User groups and characteristics**	**Enabling affordances & goal(s) oriented action**	**Constraining affordances**	**Outcome(s) and key reflections**	**IS streams that could contribute towards de-escalation**
A1: Contact initiation and communication through proxy identities [TIDM – Stage 1]	Social Networking sites and web-applications	*Offenders* have the ability to connect with children by masking their real identity.	Find children online and communicate with them	Only known sex offenders are constrained in initiating contact or those imprisoned	Communication with children is established easily as the real identity of the offender is masked	Online identity, age-restriction information systems management
Shared affordance (between offenders and police officers, online vigilantes)		*(1) Police officers* will mask their identities online similar tactics and 'reverse-engineer' the online behaviour of offenders. This constraint applies also to *(2) Online vigilantes* (individuals or groups)	Impersonate children online and communicate, expose, and pursue offenders	Legally bounded technology-use Unwitting disruption or interference of legitimate cybercrime police operations (by vigilantes)	Ability to lure offenders into activities that expose their behaviour and identify them for arrests, confiscation of devices, digital forensics and pursue prosecution.	AI, Machine Learning, Cognitive Chatbots (e.g. bots emulating cybercrime agents), Advanced Honeypot Techniques, Security
A2: Trust development through digital imagery [TIDM – Stage 2]	Social networks, web-apps, image-editing software, face-swap apps, AI-deepfakes	*Offenders* have the ability to use nude imagery in social networks and other applications in order to gain the (initial) trust of the victims and persist over time until that trust is elevated (often by offering nude imagery first)	Generate photorealistic imagery; communicate such imagery through social networks; use real child pornography to attract further victims	Real-time nude imagery detection in some applications can be triggered to constrain offender goal in creation and/or communication of imagery	Children trust offenders and become compliant to demands while deceived by the use of fake imagery supporting the digital identity of the offender.	Hardware/Software based image detection and blocking, trust and digital identity, Identity Management Systems, IS management of large-scale image analytics
A3: Engage in online extortion and receive 1st generation imagery [TIDM – Stage 3]	Hardware and cloud-based storage devices, social networks, web-apps	*Offenders* communicate with victims and once the latter have offered imagery, offenders will threaten them and put them in a suspended state of extortion	Receive and store child pornography online; Establish/maintain the continuous supply of imagery by using extortion tactics & store such imagery	Real-time nude imagery detection in some applications can be triggered to constrain offender goal in receiving imagery	Children feel forced to offer nude imagery under extreme pressure and threats (e.g. death threats to family members) while the volume of imagery escalates	Deep learning (conversational analysis), digital forensics, cloud-based forensics
A4: Traffic child imagery, encrypt imagery and explore elite networking or monetization/gamification [ITDM – Stage 4] ***Shared affordance*** (for trafficking)	P2P networks, dark-web, elite online paedophile forums, cryptocurrencies, digital tokens	*Offenders* communicate with other offenders to exchange imagery. They can also encrypt imagery and explore other exchange-oriented forms (e.g. elite networks and gamify/monetise online CSE)	Enhance collection of imagery by participating in trafficking networks, join elite pornographic networks, monetize exchange activities	Network-based detection on hashed 2nd generation imagery, group-infiltration	Child pornography becomes widely distributed. Imagery acquires digital value and monetization in cryptocurrencies like Bitcoin or virtual	P2P Network monitoring, Digital Forensic Management, Online Underground Markets, Cyber-Money Laundering, Organisational IS Cross-Border IS/IT collaboration,

Collective affordance (for elite networking with differential use)					tokens (e.g. paedopoints) occurs; underground markets and gamification	Organisational Learning, Governance and Organisational structures
A5: Identify 2nd generation imagery and differentiate them from 1st generation	INFOTRACK, CAID, PhotoDNA – Microsoft	*National Crime Agency users* and *CCU users* rely on this IS to identify 2nd generation imagery *Police Officers* in the field will have additional demands so that PhotoDNA and associated tools can be used (e.g. photograph empty rooms of suspects to link historical online CSE cases)	Monitor P2P networks for files being exchanged and separate 2nd generation imagery by using hashed values Re-classify spurious 1st generation imagery as 2nd generation that is not high-risk or time-sensitive. Link offender to multiple victims in historical cases	Not a permanently on connection and restricted by the overwhelming data deluge created in online networks. User-familiarity and re-allocation creates additional constraints (e.g. in customization of filters)	(1) Prioritize 1st gen. imagery and recognize victims faster by eliminating 2nd generation images (2) Identify suspects/block the exchange or search for 2nd generation imagery through technology companies	Information management of image-recognition, network monitoring, P2P monitoring and analysis
A6: Combine intelligence from different sources and build up offender profiles ***Collective affordance*** (differential use based on user experience)	HOLMES 2 and other IS; TARGET (profiling) and INITIATE (triage)	Cybercrime Police officers Awareness of distributed intelligence and/or missing intelligence	Build offender profiles from multiple sources in order to prioritise cases	Data quality issues, perception of poor ability to combine intelligence in a timely fashion and stark interoperability concerns	The problems created by interoperability make it very difficult in some cases to build comprehensive offender profiles.	Interoperability at different IS levels (technical, formal/policy-oriented, semantic), recommend
A7: Conduct time-sensitive scan on imagery and risk score contact sex offenders ***Shared affordance*** (CCU users conduct this in similar ways)	INITIATE (triage), HARVEST (real-time filtering), TARGET (risk),	CCU Users operating the INITIATE (IS) for Triage purposes will prioritise the high-risk cases (also with the help of TARGET and forward those for full forensic analysis	Collect enough imagery to secure prosecution (e.g. under UK law, 50 class A photographs)	Missed 1st generation imagery due to filtering restrictions and volume demands Backlog of triage analysis, outsourcing/financial implications	Children that are victims might be missed due to algorithmic/profiling restrictions while volume of data makes triage necessary and might create backlogs	Risk-based approaches to online CSE assessment, IS compliance and certification, outsourcing, behavioural profiling
A8: Prioritize vulnerable children at school	School Filtering Information Systems	*IT analysts in school IT departments* ability to conduct monitoring of the online searches of children via school IT infrastructure	Prioritize children that are more vulnerable for online CSE at school	Inability to process all red flags due to their sheer volume.	The way children use technology at school can provide early-warning vectors of future victimization but these monitoring tools place demands on manual analysis	Privacy and data sharing, Behavioural IS Security, User-controlled privacy, Privacy Enhancing Technologies in Software, Cyber-awareness, Privacy by Design, Online Trust

A9: Posting children's photographs online ***Misperceived Affordance***	Social network accounts of parents School Twitter/Facebook accounts Children's social networking accounts	*Parents* share imagery of children with online friends and family. *Schools* also share online for promoting their activities *Children* share their own imagery (often bypassing the age-notifications)	Unintentional image-(over)sharing by parents, children and other stakeholders (e.g. schools) can lead to exploitation and fuels imagery manipulation	While parents do not face restrictions in this goal-oriented action, user appropriate warnings based on image recognition could be	(1) Child imagery is captured, distorted, sexualized and re-circulated as online pornography (2) Children become desensitized towards online privacy (3) Comingling of imagery creates detection challenges	Cybersecurity-awareness, Online safety, Privacy and data sharing, Behavioural IS Security, User-controlled privacy, Risk Management, , Privacy by Design, Online Trust
A10: Monitor online conversations for suspicious keywords	HARVEST IS	*Cybercrime analysts* have the ability to develop offender profiles and launch them for offender-monitoring in online forums.	Listen to social media conversations in real-time *and* apply keyword filters to identify offenders	Large numbers of false positives, lengthy/complex investigative trails and associated costs made this approach unsustainable	Information system was shut down due to number of false-positives and lack of resources but worthy of future exploration.	AI and autonomous agents, Large-scale social media monitoring, Privacy/Security balancing, Profiling, Risk, Filtering, Software Development & Design, Algorithmic Accountability
A11: Bypass encryption on confiscated devices	REVERSE IS (decryption)	*Digital forensics analysts* will use specialist hardware/software combinations in order to decrypt confiscated devices	Bypass encryption on mobile phones and other devices by reverse (social) engineering security and/or brute-force attacks	Constrained by what can be achieved with brute force attack, hardware-assisted & software decryption tools relying on collected intelligence in the field	If access is not secured, section 49 of the RIPA code can be used (but is rarely used as it is a costly legal route demanding national approval)	Digital Forensics, Data filtering for prioritization, Compliance and Legal Implications of IS-use, Cloud-based Forensics
A12: Access social media accounts by bypassing age-restrictions ***Misperceived Affordance***	Social networks, web/mobile-applications	*Children* gain access to social networks at a very young age	Gain access to social networks by bypassing age-restrictions and establish online relationships; gain popularity	Constrained if/when age-restriction tools cannot be bypassed, or parental controls	The ability of children to bypass age-restriction tools allows them to connect online but they do not realize the severity of the dangers they're exposed to	Cyber-security awareness, online identity management

Table 3: Affordances of online CSE

DISCUSSION ON AFFORDANCES

While technological affordances have both enabling and constraining expressions as shown in Table 3, the multi-dimensionality and interconnectedness of affordances points to a problem that is truly difficult to untangle. This article makes a first attempt towards deconstructing the role of technology and imagery in online CSE from an IS perspective. It is important to assert that IS research can make a difference in two ways: a) by focusing on studies around the in-actualisation of the enabling affordances for offenders, and of course, by increasing, strengthening, and inventing new constraining affordances for offenders (so that their goal to lure children through technology-use is disrupted), b) by strengthening the enabling affordances for cybercrime teams and minimising their constraining affordances; here, the study of different cybercrime teams and jurisdictions could shed some valuable light. The study of the broader organisational IS context within which cybercrime teams are embedded is also significant as we have shown in our analysis. The same applies to the critical role of technology providers, and in particular, social networking companies; a deeper exploration of their organisational dimensions and a clearer understanding of the problems, challenges, and missed opportunities that they face in tackling the phenomenon would lead to additional lines of scholarly inquiry. A longitudinal in-depth case study of a major social networking company would be invaluable in this context. Overall, our organisation of affordances in Table 3 can assist IS scholars in concentrating their lines of exploration further.

Through our empirical findings we delineate several ways through which technology is used by offenders to fulfil their goal-oriented actions. By using social networking sites, web-applications,

image editing software, face-swap applications, AI-based deepfakes, P2P networks, the dark-web, cloud-storage, as well as elite forums that are supported by underground digital economies and cryptocurrencies (or custom-made digital tokens), offenders are quick to adopt new technologies to enable their illegal goals to lure children online. The technology artefacts involved, the corresponding user-characteristics of offenders, the enabling/constraining affordances and the corresponding outcomes are listed in Table 2 while the centrality of imagery across many affordances is evident. By bringing together the insights of our preliminary model (depicting only the offenders' side), the organisational insights from studying the CCU and the extracted affordances in Table 3, we reconceptualize and describe our comprehensive model (Figure 3), depicting both the offenders and the CCU's sides.

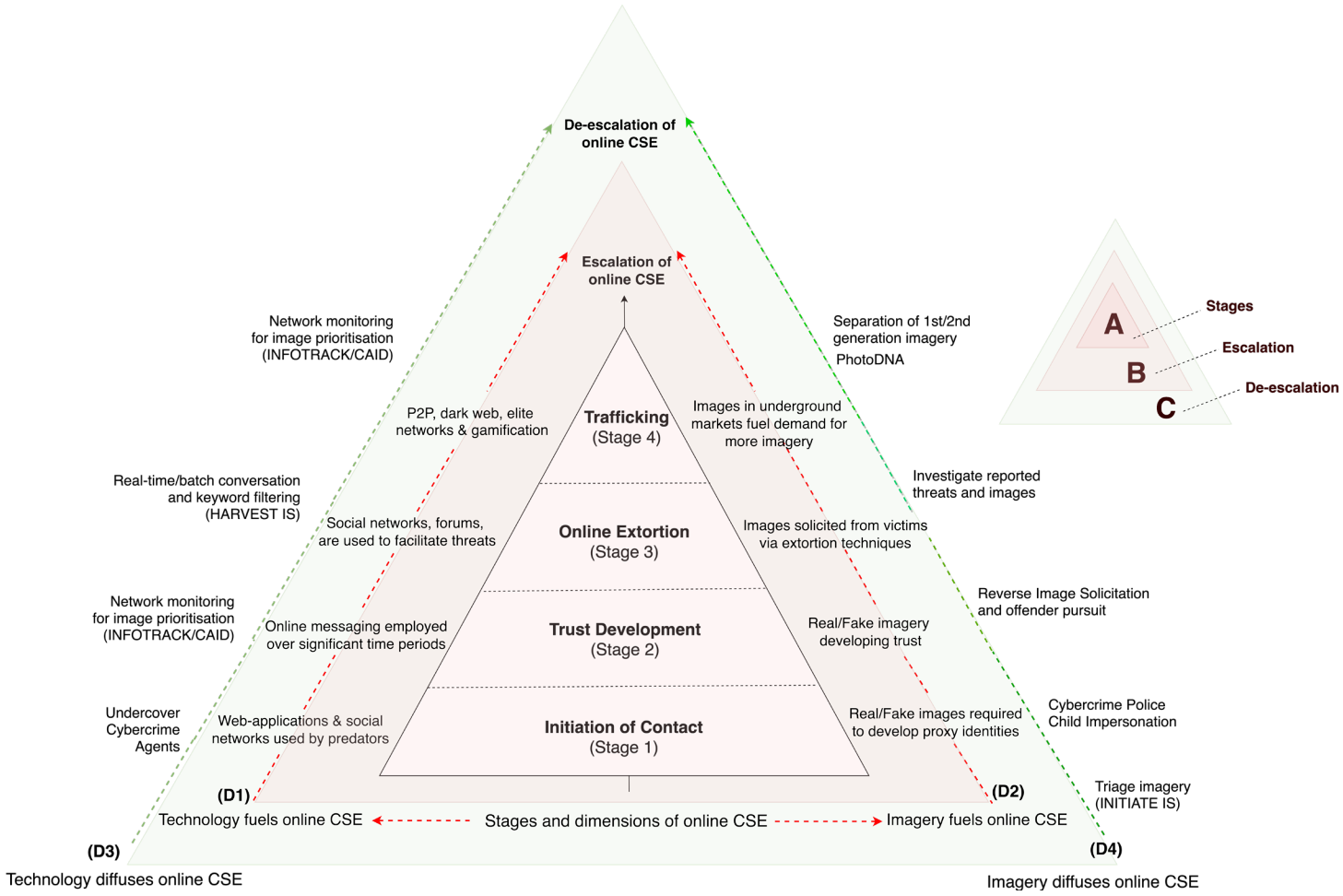


Figure 3: The Technology and Imagery Dimensions Model (TIDM)

The nested triangles A, B, and C in Figure 3 both summarize and generalize what we have learned about online CSE. The left side of the triangle illustrates how properties of *technology* shape how users may interact with them. The right side shows how properties of *imagery* invite users to act in various ways. Below, we describe the nested triangles briefly before we discuss the affordances.

A. Stages of online CSE: The centre triangle of Figure 3 shows the various stages of online CSE. These are 1) initiation of contact, 2) trust development, 3) online extortion and 4) trafficking.

B. Escalation of online CSE: The second triangle of Figure 3 represents how *offenders* make use of the enabling affordances of technology and imagery; the goal-oriented action of the offenders results in the escalation of online CSE. Of course, for each stage, offenders are limited by the constraining affordances of the corresponding artefacts (see Table 3). But overall, it is the enabling affordances here that contribute to the escalation of the phenomenon as captured by D1 and D2 of the diagram alongside all four stages of online CSE.

C. De-escalation of online CSE: The outermost triangle represents the complicated actions of how cybercrime police (or in some cases, vigilantes), make use of the affordances of technology and imagery so that they can de-escalate online CSE. Like the perpetrators, these parties are limited by the constraining affordances of artefacts.

A number of IS streams can be associated with in-actualizing the enabling affordances of artefacts for offenders and dampening their effects. Image analytics (Vuppala *et al.*, 2018), trust and digital identity (Halperin and Backhouse, 2012), deconstructing the dark side of social media (Baccarella *et al.*, 2018), the study of online underground markets and cyber-money laundering (Philippsohn, 2001; Demetis, 2018) are all important, but they need to be concentrated onto disrupting online CSE. A more targeted focus on the handling of digital forensics (Garfinkel, 2010) in the context of online CSE is also necessary. Organisational IS have a lot to contribute in this space as we observed and discussed several organisational/IS barriers that create limitations in the sharing of intelligence and in the prioritisation of cases. Interoperability concerns, risk-

based approaches and communication disconnects within the Police are all worthy of further exploration.

Our empirical data also points to misperceived affordances. While these affordances are not perceived by the user groups, they do exist (Gaver, 1991). For example, the misperceived affordance (A9 in Table 3) captures that possibility of unintentional image-(over)sharing by parents, children and other stakeholders (e.g. schools) that can lead to exploitation. Such imagery is captured, distorted, sexualized and recirculated as online pornography; the desensitization of children towards online privacy and the comingling of imagery creates further detection challenges. The field of IS offers a number of streams in this context. A focus on privacy and data sharing already exists (Furnell, 2015), much like on behavioural IS security (Dhillon, Syed and Pedron, 2016), user-controlled privacy in relation to mobile phones and Privacy Enhancing Technologies (PETs) (ENISA, 2015) and cyber-awareness (Franke and Brynielsson, 2014). But thus far, these streams have not focused on online CSE; doing so could create invaluable contributions towards the de-escalation of the phenomenon. Design implications will demand further exploration toward these goals.

While systemic difficulties in handling these aspects create severe challenges for the future, still, even in the face of such adversity, a number of distinct ways can be identified in which technology enables the de-escalation of the phenomenon, despite several constraints (e.g. handling encryption, resourcing problems, interoperability concerns, etc). For example, the identification of previously circulated (2nd generation) imagery through the INFOTRACK system and the CAID database enable the prioritisation of 1st generation imagery and the recognition of potentially live-cases at a much faster pace (A5 in Table 2). More IS research in this context in

peer-to-peer network monitoring and filtering (Weber, 2016), darknet monitoring (Nunes *et al.*, 2016) and digital forensics can yield considerable insights through which this can be reinforced.

Similarly, the use of behavioural profiling and other filtering approaches to risk-score the severity of offenders (A7) and the vulnerability of children can assist cybercrime authorities to cease the ongoing exploitation of victims. Profiling (Lamb and Kling, 2003; Middleton, Shadbolt and De Roure, 2004) and its closely associated risk prioritisation and management (Spears and Barki, 2017), as well as the development of software that can enable such prioritization need to be considered. A subtler point arises here with the algorithms that conduct such prioritisations since associated criminal investigations can be triggered by who is flagged as more highly suspect. Particularly in occasions where algorithmic transparency is very difficult, if not impossible to achieve (e.g. due to 'black box' approaches like machine learning), one can speak of the technological construction of suspicion. Thus, algorithmic accountability in this context acquires a particular significance (Garfinkel *et al.*, 2017).

Another significant de-escalation potential comes from the work being conducted in order to gain access to offender devices and accounts (both cloud-based and confiscated devices) (A11). The work of cybercrime authorities can make a substantial difference in safeguarding children; cloud-based and digital forensics, as well as data filtering for prioritization are two indicative IS streams that can strengthen that enabling affordance for the Police. Unfortunately, encryption is also enabling offenders to protect their digital assets and this remains a battleground between encryption-focused offenders and decryption-focused digital forensic specialists. The context of balancing the strengthening of encryption and its exploitation by offenders with the decryption capacities of cybercrime units remains truly challenging.

Even though in our discussion we saw several IS at the CCU that contribute towards the de-escalation of the phenomenon and the pursuit of offenders, we would like to highlight the ability of cybercrime agents and online vigilantes[8] to conduct impersonations of children themselves in order to expose offenders. While the process of having police officers luring offenders by impersonating children online can be time consuming, the use of social networks to enable to expose offenders is shared with online vigilantes and their users. As we saw in our description in the previous section, an automated replication of this process has been attempted through the HARVEST IS where online conversations for offender identification (A10 in Table 2) were monitored by listening to social media conversations in real-time. While this was shut down due to the sheer number of false-positives, a variety of other computational approaches can be explored toward that end. Advanced "honeypot techniques" with digital tokens (Shabtai *et al.*, 2016), machine learning (Pearl, 2019), or AI-based chatbots (Androutsopoulou *et al.*, 2019) that could in the future be taking over the role of undercover cybercrime agents and posing as children online. Overall, we do perceive the role of AI as having a set of potentially critical effects for both escalating and de-escalating the phenomenon. We prompt other IS scholars to explore these in detail; for example, deepfakes and AI-based face/voice mimicking would allow offenders to attract more victims and more artificial identities more convincing and realistic, while better detection tools might expose such deepfakes and alert users (an AI *vs* AI scenario).

[8] Formally, the Crown Prosecution Service will warn against online vigilantes for online CSE as they might endanger themselves, interfere with formal Police investigations, and break the law if the participate in the crime and receive imagery.

Similarly, AI developments might assist police if autonomous software-based cybercrime agents can be launched online and try to discuss with/expose offenders autonomously before referring them for a manual cybercrime review; could support this significant potential.

RESEARCH DIRECTIONS FOR THE FUTURE, LIMITATIONS AND CONCLUSIONS

By using a grounded theory approach and developing a model (TIDM) to depict the staging of online CSE in relation to imagery and technology while contextualizing it in an organisational context, as well as by organizing the technology affordances around online CSE, this article contributes to our deeper understanding of the phenomenon. Its complexity, the multiplicity of IS-related considerations and the enormous social impact attached to online CSE must prompt other IS scholars to engage with it.

While an obvious path for further research would be a deeper exploration across the affordances organised in Table 3, there are a number of additional questions we would like to raise. What online behavioural patterns can alert us to a higher probability that a youngster may be targeted (due to their online behaviour)? Can (and should) technology companies use vulnerable social interaction filtering to flag potential vulnerabilities in how children use technology (like banks use suspicious transaction filtering software to flag potential suspects for illegal behaviour (e.g. money laundering, fraud, etc.)? If so, what would be the indicators/proxies of online behavioural vulnerability for children over time? What are the privacy considerations attached to such monitoring?

The above considerations raise several additional research questions that are ripe for research: how do dark web affordances enable and constrain the activities of offenders and the

CCU? A dark-web based study could yield significant insights. What is the role of crypto-currencies, like bitcoin, in facilitating transactions for underground markets? How do online predators seek collaboration through online ecosystems/networks and how can P2P monitoring be strengthened for real-time filtering of suspicious online CSE behaviour?

Also, as internet users, children violate terms and conditions (of age-limit) routinely. Can this violation be inferred by the semantic analysis of the texts/posts being sent by children as a preventative measure? What monitoring mechanisms can social networking companies develop for such behaviour? In-depth case studies of social media and other technology companies that attempt to tackle this phenomenon would help elevate our understanding on the challenges of tackling online CSE under the difficult data deluge conditions we describe. Furthermore, while IS research has focused on online trust on various fronts, the dark side of online trust and what this means for phenomena like online CSE raises important questions. What are the qualitative differences between offenders that attempt to establish a deception-oriented online trust between them and stakeholders in other contexts that seek to establish true online trust? Would a comparison between online CSE and online SE (of adults) expose further interesting differentiations that could yield better results?

Finally, the overall handling of online CSE and the way the phenomenon itself has emerged and evolved, raises several ethical considerations. In this spirit, there is a rich literature at the intersection of ethics & IS that can be applied in order to unpack the ethical dimensions of the phenomenon. Classical theories in ethics and more contemporary information ethics (Floridi, 2008) can probe further important questions on the values in technology, personal values in computer ethics, rights of algorithms in monitoring/filtering sensitive phenomena like online

CSE and the ethics of IT-artefacts themselves. An ethical deconstruction of the phenomenon would also help us probe the conditions under which more invasive profiling/monitoring of online CSE can be conducted in order to safeguard children.

Online CSE is a serious and complex phenomenon with multiple IS-dimensionalities. We hope that our study motivates other scholars in our discipline, and in others, to explore this phenomenon further. We hope that our article encourages all readers (as researchers, members of law-enforcement, policy-makers, systems developers and parents) to take every possible opportunity to participate in the fight against online CSE.

REFERENCES

Akullo, M. (2012) 'Child-trafficking policymaking between Africa and Europe', in Lawrance, B. N. and Roberts, R. L. (eds) *Trafficking in Slavery's Wake: Law and the Experience of Women and Children*. Ohio University Press, pp. 184–204. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84906124233&partnerID=40&md5=53a2d3660ff73873f2a6b1b6849e9f8e.

Alexy, E. M., Burgess, A. W. and Baker, T. (2005) 'Internet offenders traders, travelers, and combination trader-travelers', *Journal of Interpersonal Violence*, 20(7), pp. 804–812. doi: 10.1177/0886260505276091.

Alvesson, M. and Sandberg, J. (2011) 'Generating research questions through problematization', *Academy of Management Review*, 36(2), pp. 247–271. doi: 10.5465/amr.2009.0188.

Androutsopoulou, A. *et al.* (2019) 'Transforming the communication between citizens and government through AI-guided chatbots', *Government Information Quarterly*, 36(2), pp. 358–367. doi: 10.1016/j.giq.2018.10.001.

Baccarella, C. V. *et al.* (2018) 'Social media? It's serious! Understanding the dark side of social media', *European Management Journal*, 36(4), pp. 431–438.

Barnard-Wills, D. (2012) 'E-safety education: Young people, surveillance and responsibility', *Criminology and Criminal Justice*, 12(3), pp. 239–255. doi: 10.1177/1748895811432957.

Bartels, R. M. and Merdian, H. L. (2016) 'The implicit theories of child sexual exploitation material users: An initial conceptualization', *Aggression and Violent Behavior*, 26, pp. 16–25. doi: 10.1016/j.avb.2015.11.002.

Battersby, L. (2015) *Millions of social media photos found on child exploitation sharing sites* . Available at: http://www.smh.com.au/national/millions-of-social-media-photos-found-on-child-exploitation-sharing-sites-20150929-gjxe55.html.

Breeden, B. and Mulholland, J. (2006) 'Investigating "Internet Crimes Against Children" (ICAC) cases in the state of Florida', in *Proceedings of the ACM Symposium on Applied*

Computing , pp. 288–292. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-33751051543&partnerID=40&md5=7cdc04c7c9c601162bdc03f8eb16e03a.

Calcara, G. (2013) 'The role of interpol and Europol in the fight against cybercrime, with particular reference to the sexual exploitation of children online and child pornography', *Masaryk University Journal of Law and Technology*, 7(1), pp. 19–33. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84882974901&partnerID=40&md5=2e4f598a86e55644dc6d1f4c0d50edd8.

Carr, A. (2013) 'The social dimension of the online trade of child sexual exploitation material', in Quayle, E. and Ribisl, K. (eds) *Understanding and Preventing Online Sexual Exploitation of Children*, pp. 96–115. doi: 10.4324/9780203127766.

Charmaz, K. (2014) *Constructing Grounded Theory: Second Edition*, *Constructing Grounded Theory*. Sage Publications.

Corbin, J. and Strauss, A. (2007) *Basics of qualitative research: Techniques and procedures for developing grounded theory.* Sage publications.

Creswell, J. (2013) *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Demetis, D. S. (2018) 'Fighting money laundering with technology: A case study of Bank X in the UK', *Decision Support Systems*, 105, pp. 96–107. doi: 10.1016/j.dss.2017.11.005.

Dhillon, G., Syed, R. and Pedron, C. (2016) 'Interpreting information security culture: An organizational transformation case study', *Computers and Security*, 56, pp. 63–69. doi: 10.1016/j.cose.2015.10.001.

Dowdell, E. B. and Bradley, P. K. (2010) 'Risky Internet behaviors: A case study of online and offline stalking', *Journal of School Nursing*, 26(6), pp. 436–442. doi: 10.1177/1059840510380209.

Eisenstein, E. (2013) 'Digital generation and sexuality development', *Adolescencia e Saude*, 10(SUPPL. 1), pp. 61–71. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84892407881&partnerID=40&md5=1734e92bbd54d4094c5168fd0e402066.

Elliott, I. and Beech, A. (2009) 'Understanding online child pornography use: Applying sexual offense theory to internet offenders', *Aggression and Violent Behavior*, 14(3), pp. 180–

193.

ENISA (2015) *Privacy and Data Protection by Design - from policy to engineering*, *Cryptography and Security*. doi: 10.2824/38623.

Etzioni, A. (2015) 'NSA: National Security vs. Individual Rights', *Intelligence and National Security*, 30(1), pp. 100–136. doi: 10.1080/02684527.2013.867221.

Floridi, L. (2008) 'Information ethics: A Reappraisal', *Ethics and Information Technology*. doi: 10.1007/s10676-008-9176-4.

Franke, U. and Brynielsson, J. (2014) 'Cyber situational awareness - A systematic review of the literature', *Computers and Security*, 46, pp. 18–31. doi: 10.1016/j.cose.2014.06.008.

Furnell, S. (2015) 'Managing privacy settings: Lots of options, but beyond control?', *Computer Fraud and Security*, 2015(4), pp. 8–13. doi: 10.1016/S1361-3723(15)30027-0.

Garfinkel, S. *et al.* (2017) 'Toward algorithmic transparency and accountability', *Communications of the ACM*, 60(9). doi: 10.1145/3125780.

Garfinkel, S. L. (2010) 'Digital forensics research: The next 10 years', *Digital Investigation*, 7, pp. S63–S73. doi: 10.1016/j.diin.2010.05.009.

Gaver, W. (1991) 'Technological Affordances', in *Proceedings of CHI 1991*.

Gibson, J. J. (1977) 'The theory of affordance', in *Perceiving, Acting, and Knowing: Toward an Ecological Psychology*.

Glaser, B. G. (1978) 'Theoretical sensitivity: Advances in the methodology of grounded theory.', *Sociology Pr.* doi: Casa.

Glaser, B. and Strauss, A. (1967) 'Applying Grounded Theory. The discovery of grounded theory: strategies of qualitative research', *The Grounded Theory Review*.

Guan, J. and Huck, J. (2012) 'Children in the digital age: Exploring issues of cybersecurity', in *ACM International Conference Proceeding Series*, pp. 506–507. doi: 10.1145/2132176.2132266.

Halperin, R. and Backhouse, J. (2012) 'Trust, Risk, and eid: Exploring public perceptions of digital identity systems', *First Monday*, 17(4).

Heurix, J. *et al.* (2015) 'A taxonomy for privacy enhancing technologies', *Computers and Security*, 53(C). doi: 10.1016/j.cose.2015.05.002.

Hillman, H., Hooper, C. and Choo, K. K. R. (2014) 'Online child exploitation:

Challenges and future research directions', *Computer Law and Security Review*, 30(6), pp. 687–698. doi: 10.1016/j.clsr.2014.09.007.

Hutchby, I. (2001) 'Technologies, Texts and Affordances', *Sociology*. SAGE Publications, 35(2), pp. 441–456. doi: 10.1177/s0038038501000219.

Jalil, J. A. (2015) 'Combating child pornography in digital Era: Is Malaysian law adequate to meet the digital challenge?', *Pertanika Journal of Social Science and Humanities*, 23(October), pp. 137–152. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84943648115&partnerID=40&md5=d71737896563e6772892914218cc3bf4.

Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). Deepfakes: Trick or treat?. *Business Horizons*, *63*(2), 135-146.

Klein, H. and Myers, M. (1999) 'A set of principles for conducting and evaluating interpretive field studies in information systems. ', *MIS Quarterly*, 23(1), pp. 67–94.

Lamb and Kling (2003) 'Reconceptualizing Users as Social Actors in Information Systems Research', *MIS Quarterly*, 27(2), pp. 197–235. doi: 10.2307/30036529.

Lee, J. K. (2015) 'Research Framework for AIS Grand Vision of the Bright ICT Initiative', *MIS Quarterly*, 39(2), pp. iii–xii.

Leonardi, P. (2013) 'A comparative study of feature use and shared affordances', *MIS Quarterly*, 37(3), pp. 749–755.

Livingstone, S. (2008) 'Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression', *New media & society*, 10(3), pp. 393–411.

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), pp. 23–32. doi: 10.1300/J070v16n02_02.

Marcum, C. D., Ricketts, M. L. and Higgins, G. E. (2010) 'Assessing sex experiences of online victimization: An examination of adolescent online behaviors using routine activity theory', *Criminal justice review*, 35(4), pp. 412–437.

Markus, L. and Silver, M. (2008) 'A Foundation for the Study of IT Effects: A New Look at DeSanctis and Poole's Concepts of Structural Features and Spirit', *Journal of the Association for Information Systems*, 9(10), pp. 609–632.

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), pp. 96–115. doi: 10.1080/0145935X.2014.924334.

Martin, P. and Turner, B. (1986) 'Grounded theory and organizational research', *The Journal of Applied Behavioral Science*, 22(2), pp. 141–157.

McCarthy, J. A. (2010) 'Internet sexual activity: A comparison between contact and non-contact child pornography offenders', *Journal of Sexual Aggression*, 16(2), pp. 181–195. doi: 10.1080/13552601003760006.

Middleton, S. E., Shadbolt, N. R. and De Roure, D. C. (2004) 'Ontological user profiling in recommender systems', *ACM Transactions on Information Systems*, 22(1). doi: 10.1145/963770.963773.

Miller, T. W. and Veltkamp, L. J. (1998) 'Clinical handbook of adult exploitation and abuse.', *Clinical handbook of adult exploitation and abuse.*

Mitchell, K. J. *et al.* (2010) 'Growth and change in undercover online child exploitation investigations, 2000-2006', *Policing and Society*, 20(4), pp. 416–431. doi: 10.1080/10439463.2010.523113.

NCA (2019) *National Strategic Assessment of Serious & Organised Crime*, *National Strategy of the NCA*. Available at: https://nationalcrimeagency.gov.uk/who-we-are/publications/297-national-strategic-assessment-director-general-lynne-owens-speech/file.

Nunes, E. *et al.* (2016) 'Darknet and deepnet mining for proactive cybersecurity threat intelligence', in *IEEE International Conference on Intelligence and Security Informatics: Cybersecurity and Big Data, ISI 2016*. doi: 10.1109/ISI.2016.7745435.

Orlikowski, W. (1993) 'CASE tools are organizational change: Investigating Incremental and Radical Changes in Systems Development', *MIS Quarterly*, 17(3), pp. 309–340.

Owens, J. N. *et al.* (2016) 'Investigative aspects of crossover offending from a sample of FBI online child sexual exploitation cases', *Aggression and Violent Behavior*, 30, pp. 3–14. doi: 10.1016/j.avb.2016.07.001.

Pearl, J. (2019) 'The seven tools of causal inference, with reflections on machine learning', *Communications of the ACM*, 62(3). doi: 10.1145/3241036.

Philippsohn, S. (2001) 'Money Laundering on the Internet', *Computers & Security*, 20,

pp. 485–490.

Quayle, E. and Newman, E. (2015) 'The Role of Sexual Images in Online and Offline Sexual Behaviour With Minors', *Current Psychiatry Reports*, 17(6). doi: 10.1007/s11920-015-0579-8.

Richards, V. (2015) *Paedophile websites steal half their photos from social media sites like Facebook*. Available at: http://www.independent.co.uk/news/world/australasia/paedophile-websites-steal-half-their-photos-from-social-media-sites-like-facebook-a6673191.html.

Shabtai, A. *et al.* (2016) 'Behavioral study of users when interacting with active honeytokens', *ACM Transactions on Information and System Security*, 18(3). doi: 10.1145/2854152.

Smith, A. M. (2014) 'Protection of children online: Federal and state laws addressing cyberstalking, cyberharassment, and cyberbullying', in *Student Bullying: Federal Perspectives and Reference Materials*, pp. 39–84. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84948406668&partnerID=40&md5=39acf28af11fd3f5d0eca922b2811e73.

Spears and Barki (2017) 'User Participation in Information Systems Security Risk Management', *MIS Quarterly*, 34(3), pp. 503–522. doi: 10.2307/25750689.

Strauss, A. and Corbin, J. (1998) *Basics of qualitative research*. Thousand Oaks, CA: Sage.

Tener, D., Wolak, J. and Finkelhor, D. (2015) 'A typology of offenders who use online communications to commit sex crimes against minors', *Journal of Aggression, Maltreatment and Trauma*, 24(3), pp. 319–337. doi: 10.1080/10926771.2015.1009602.

UKGov (2015) *Fact Sheet 2: National Security Risk Assessment*. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62484/Factsheet2-National-Security-Risk-Assessment.pdf.

Volkoff, O. and Strong, D. (2018) 'Affordance theory and how to use it in IS research', *The Routledge Companion to Management Information Systems*.

Volkoff, O. and Strong, D. M. (2013) 'Critical realism and affordances: Theorizing IT-associated organizational change processes', *MIS Quarterly: Management Information Systems*, 37(3). doi: 10.25300/MISQ/2013/37.3.07.

Vuppala, S. K. *et al.* (2018) 'Cloud Based Big Data Platform for Image Analytics', in *Proceedings - 2017 IEEE International Conference on Cloud Computing in Emerging Markets, CCEM 2017*. doi: 10.1109/CCEM.2017.11.

Walsham, G. (1995) 'The Emergence of Interpretivism in IS Research', *Information Systems Research*, 6(4), pp. 376–394. doi: 10.1287/isre.6.4.376.

Weber, T. A. (2016) 'Product Pricing in a Peer-to-Peer Economy', *Journal of Management Information Systems*, 33(2). doi: 10.1080/07421222.2016.1205933.

von Weiler, J., Haardt-Becker, A. and Schulte, S. (2010) 'Care and treatment of child victims of child pornographic exploitation (CPE) in Germany', *Journal of Sexual Aggression*, 16(2), pp. 211–222. doi: 10.1080/13552601003759990.

Wells, M. and Mitchell, K. (2008) 'How do high-risk youth use the Internet? Characteristics and implications for prevention', *Child Maltreatment*, 13(3).

Wolak, J., Liberatore, M. and Levine, B. N. (2014) 'Measuring a year of child pornography trafficking by U.S. computers on a peer-to-peer network', *Child Abuse and Neglect*, 38(2), pp. 347–356. doi: 10.1016/j.chiabu.2013.10.018.

APPENDIX 1

<table>
<tr><td colspan="6">Problematisation for the phenomenon of online CSE</td></tr>
<tr><td colspan="6">Typology of assumptions open for problematisation</td></tr>
<tr><td>Inhouse

Key assumptions include: a) its escalation due to underground markets, b) offender approaches to coercion, c) children targeting and availability of online information, d) the key role between parents and children, e) online behaviour</td><td>Root metaphor

By deceiving and luring children online through a variety of platforms and social networks, offenders can victimise children online and gain access to child pornographic imagery (for their own use or for P2P exchanges)</td><td colspan="2">Paradigm based

The development of different classifications for internet offenders (e.g. travellers/traders) seems to play a key role in different research approaches around the phenomenon. How we know what we know about the phenomenon seems to be intertwined around classifications and offender attitudes as well as offender/victim interaction but an IS perspective is missing</td><td>Ideology

Without a doubt, tackling online CSE is a morally charged phenomenon but some aspects (e.g. role of parenting in child protection in relation to their internet behaviour) are not understood in their broader context. Gender-related assumptions sees men in the role of perpetrators; while this is largely accurate, it can create blind-spots or advanced deception tactics</td><td>Field

General assumptions shared involve: a) the critical role of imagery, b) escalation of the phenomenon, c) its security prominence, d) organisational challenges in handling it</td></tr>
<tr><td colspan="6">Principles for identifying and challenging assumptions</td></tr>
<tr><td>1. Identified domains of literature significant for online CSE

While criminology (mostly) and law have dealt extensively with online CSE, IS-research has not engaged with the phenomenon. Most work seems to concentrate on classification and developing typologies</td><td>2. Identified assumptions for the phenomenon

Key role of imagery but also online CSE as pathway to more serious offences. Detection, prevention and pursuit have many challenges</td><td>3. Evaluate articulated assumptions

Indeed, the role of imagery remains central to online CSE, however, it does not seem to be rendered onto the combined challenges of escalation/de-escalation, or indeed, into the organisational challenges of the cybercrime teams.</td><td>4. Consider alternative assumptions

The role of imagery plays a more foundational role in fuelling/ defusing the phenomenon but the scope of the enabling/constraining expressions of imagery are not well understood nor linked to an organisational context. We challenge the role of imagery by seeing it as a broader dimension of interference for online CSE (occupying different contexts, institutional efforts, organisational processes, and shaping enabling/constraining or misperceived affordances). The same applies to different technology artifacts or platforms and the way they interfere with the phenomenon.</td><td>5. Relate assumptions to audience

From politicians, to technology companies, to cybercrime teams (or even other specialised teams), stakeholder assumptions about the phenomenon (e.g. on imagery) tend to be confined in the space of their own utility but technology cuts across this phenomenon and propels sociotechnical challenges that are not well understood.</td><td>6. Evaluate alternative assumptions

A theoretical combination of staging of the phenomenon with an understanding of: a) how the phenomenon escalates, b) how cybercrime units attempt to de-escalate it, and what are the organisational challenges around it would be very interesting for bringing about a deeper understanding of online CSE from an IS perspective, be considered</td></tr>
</table>

(adapted from Alvesson and Sandberg, 2011)

APPENDIX 2

Department of Justice
U.S. Attorney's Office
Middle District of Florida

Jacksonville Man Pleads Guilty to Soliciting and Paying for Live Molestation of Children over the Internet - Jacksonville, Florida – United States Attorney A. Lee Bentley, III announces that Justin Laurence McKinley (49, Jacksonville) has pleaded guilty to sending notices over the Internet soliciting the live molestation of children for online viewing. He faces a mandatory minimum penalty of 15 years, up to 30 years, in federal prison and a potential life term of supervision.

According to court documents, in 2015, the FBI began an investigation into a website engaging in the exploitation and enticement of children to participate in sexual activity. The FBI identified several individuals located in the United States that were associated with this website. Further investigation revealed that several individuals in a foreign country were engaged in the molestation of young children for the purpose of broadcasting live streaming "sex shows" to online viewers who had paid a fee. The individuals were arrested and McKinley was identified as one of the individuals who paid to view these live streaming "sex shows." Between January 2014 and December 2015, McKinley sent a total of 100 electronic fund transfers, totalling $31,415, to the individuals who molested the children in the "sex shows."

On May 27, 2016, law enforcement officers executed a federal search warrant at McKinley's residence. During an interview, McKinley admitted that he had solicited others to molest children and live stream video of the conduct to him, and he further admitted that he had recorded many of the sessions. The victims depicted in the streaming videos ranged in age from a new-born to an 8-year-old child. Forensic analyses of McKinley's computer media revealed that a particular external hard drive contained at least 613 videos and 6,846 images depicting the sexual abuse of children. This case was investigated by the Federal Bureau of Investigation, the Jacksonville Sheriff's Office, and law enforcement authorities in several other countries. It is being prosecuted by Assistant United States Attorney D. Rodney Brown. It is another case brought as part of Project Safe Childhood, a nationwide initiative launched in May 2006 by the Department of Justice to combat the growing epidemic of child sexual exploitation and abuse. Led by United States Attorneys' Offices and the Criminal Division's Child Exploitation and Obscenity Section, Project Safe Childhood marshals federal, state, and local resources to locate, apprehend, and prosecute individuals who sexually exploit children, and to identify and rescue victims. For more information about Project Safe Childhood, please visit www.justice.gov/psc.

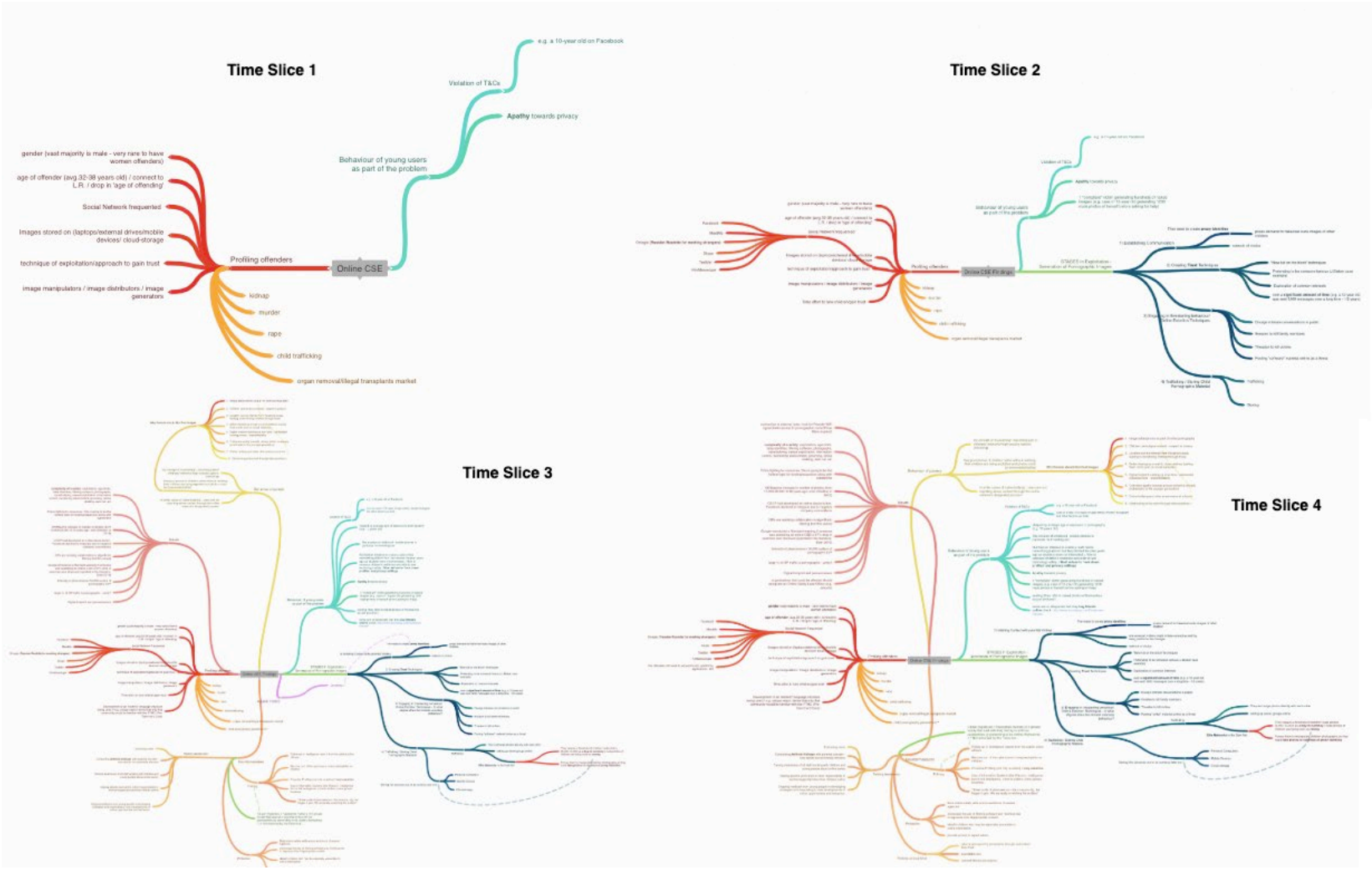
Appendix 3: Sample records from Phase 1

FBI case description on release	Image use/distribution	Social network (or other channel)	How criminals used technology	Description and user implications
MICHIGAN - A 33-year-old New Baltimore man was sentenced on Wednesday to 15 years in federal prison for producing child pornography by using Facebook to entice boys to send him nude pictures of themselves, U.S. Attorney Barbara L. McQuade announced today. Joining McQuade in the announcement was FBI Special Agent in Charge Robert D. Foley, III. On August 17, 2012, Gregory Austin, age 33, of New Baltimore, Michigan, was charged with three counts of production of child pornography for manipulating young boys, through Facebook, to create pornographic pictures of themselves. In March 2012, Austin was arrested by the Roseville Police Department in the parking lot of an elementary school for illegally purchasing Vicodin. The arrest led to an investigation that discovered images of child pornography on Austin's cellular phone. Further investigation revealed that Austin created an online persona, through Facebook, of a young woman named "Julie." Through "Julie" and her Facebook page, Austin convinced numerous minor boys, including former students, to photograph their genitals and pubic areas and send him the images. In total, 133 images, depicting mostly young boys in various states of dress and undress, were found on Austin's phone and computer. Yesterday, United States District Judge Arthur J. Tarnow sentenced Austin to 15 years in federal prison for his crimes. In making his decision, Judge Tarnow cited that Austin had committed a serious crime that required a severe punishment. Austin was also placed on five years of supervised release. According to McQuade, "Parents and teens should be aware that predators use social media to manipulate victims. This defendant tricked young boys into sending him nude pictures of themselves. You need to be careful when communicating online because you never know who really is on the other end of a digital message." The Roseville Police Department along with the Federal Bureau of Investigation's Southeast Michigan Crimes Against Children Task Force participated in the investigation and prosecution of this case. This case was brought as part of the U.S. Attorney's Project Safe Childhood, a nationwide initiative to combat the growing epidemic of child sexual exploitation through the Internet.	Fake photographs were used to create a new persona called 'Julie'. A total of 133 images were uncovered in the possession of the 33-year old including minors. There does not seem to be wider distribution.	*Facebook* was exploited to communicate in a predatory way and to trick young boys	The technique used involves *deception* mostly, relying on the creation of a fake digital identity by offenders in social media in order to entice boys to send nude pictures of themselves.	Austin created an online persona, through Facebook, of a young woman named "Julie." Through "Julie" and her Facebook page, Austin convinced numerous minor boys, including former students, to photograph their genitals and pubic areas and send him the images./ Users don't realise the permanance of data, fake identity risks, etc and send nude pictures of themselves. Caution when communicating online as the other end of a digital party can be deceptive.
OKLAHOMA CITY—Daniel Leslie Mooneyham, 33, of Oklahoma City, Oklahoma, was sentenced to 240 months in prison today by United States District Judge Timothy D. DeGiusti for receipt of child pornography depicting a 15-year-old boy, announced Sanford C. Coats, United States Attorney for the Western District of Oklahoma. According to court records, Mooneyham, using a fake Facebook profile, pretended to be an attractive, 18-year-old blonde female named "Terri Smith." Posing as Terri Smith, Mooneyham would send Facebook "friend requests" to teenage boys, some of whom he knew through a church youth group and a youth camp where he volunteered. After establishing a Facebook "friendship" with teenage boys while posing as Terri Smith, Mooneyham would solicit pictures of the boys' genitalia in exchange for sexually explicit photos of Terri Smith. Mooneyham would direct the boys to text or e-mail their nude pictures to a Yahoo! e-mail account that he had created for his Terri Smith Facebook profile. Mooneyham received nude pictures via e-mail from at least three minors and solicited others. The pictures of Terri Smith that Mooneyham sent to the boys depicted an unknown female that Mooneyham had found on the Internet. During the investigation, Mooneyham, posing as Terri Smith, also solicited a sexually explicit photo from an undercover FBI agent, who was posing as a 15-year-old boy on Facebook. When fashioning his sentence, Judge DeGiusti took into consideration evidence that, while pending sentencing, Mooneyham conspired to hire a third party to murder his wife, a plot which was ultimately foiled. His wife had reported Mooneyham's Facebook activities to the FBI, which led to his arrest. Mooneyham pled guilty on August 5, 2011. Upon release from prison, Mooneyham will be on supervised release for five years and will have to register as a sex offender. This case was part of Project Safe Childhood, the flagship program in the Department of Justice's National Strategy for Child Exploitation Prevention and Interdiction, and was the result of an investigation conducted by the Federal Bureau of Investigation, the Edmond Police Department, and the Oklahoma City Police Department. The case was prosecuted by Assistant U.S. Attorney Brandon Hale.	1) Fake images used to set up a fake profile, 2) Nude images of an unknown female were send to young boys, 3) Images were solicited from at least 3 minors, 4) Images solicited from an undercover FBI agent who was posing as a 15-y old boy on Facebook	A *Yahoo e-mail account* was used to receive the solicited photographs and *Facebook* was used to create a fake profile.	Networks are used by offenders to search for and re-use nude photographs (as a deception tactic to attract children). Social media being used to solicit images from victims and tech companies and e-mail providers (e.g. Yahoo) can be used to store images/communications	By using a fake Facebook profile, the offender pretended to be an attractive, 18-year-old blonde female named "Terri Smith." He sent Facebook "friend requests" to teenage boys, some of whom he knew through a church youth group and a youth camp where he volunteered. He would solicit pictures of the boys' genitalia in exchange for sexually explicit photos of the fake identity Terri Smith. Deceived by real nudes sourced by image-takeovers of unknown individuals, children become deceived into sharing their own nude imagery. This seems to create a recursion/self-referential loop (imagery out of imagery)

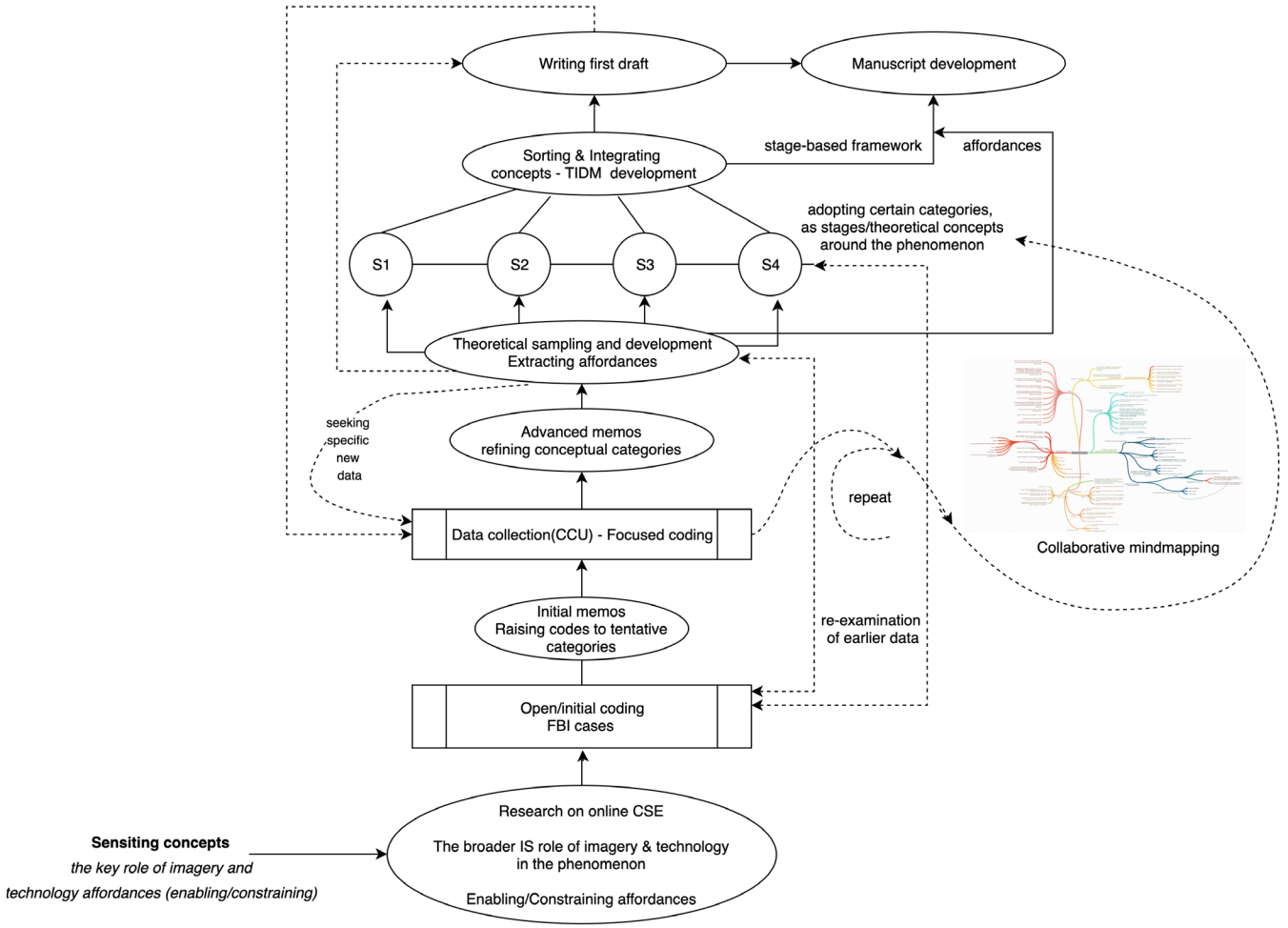
FBI case description on release	Image use/distribution	Social network (or other channel)	How criminals used technology	Description and user implications
RICHMOND, VA—Cameron Scot Bivins-Breeden, 21, of King George County, Va., pleaded guilty today to production of child pornography and enticement of a minor. Dana J. Boente, United States Attorney for the Eastern District of Virginia; and Adam S. Lee, Special Agent in Charge of the FBI's Richmond Field Office, made the announcement after the plea was accepted by United States District Judge John A. Gibney. Bivins-Breeden was indicted on April 15, 2014, by a federal grand jury on production of child pornography, in violation of 18 U.S.C. § 2251, and enticement of a minor, in violation of 18 U.S.C. § 2422. He faces a maximum penalty of life imprisonment when he is sentenced on September 22, 2014. In a statement of facts filed with his plea agreement, Bivins-Breeden admitted to enticing 38 juvenile females located across the country, ranging from 11 to 17 years old, to produce child pornography. As part of the scheme, Bivins-Breeden contacted the victims via Facebook on his iPhone posing as a juvenile female and enticed them to produce child pornography. After the juvenile victims produced the pornographic images, they sent them to Bivins-Breeden over the Internet. When the victims refused to produce additional child pornography images, Bivins-Breeden threatened to send the previously obtained images to the victims' friends, family, and schoolmates on Facebook. In total, Bivins-Breeden admitted to sending 95 child pornography images in an effort to convince victims he was, in fact, a juvenile female and causing victims to produce 45 child pornography images. This case was investigated by the Federal Bureau of Investigation. Assistant United States Attorney Erik S. Siebert and Commonwealth of Virginia, Office of the Attorney General, Assistant Attorney General and Special United States Attorney Samuel Fishel are prosecuting the case on behalf of the United States.	1) Wide number of targets attempted in order to produce images (38 juvenile females from 11 to 17 years old) 2) 95 child pornography images sent to **convince victims** that a jevenile female was contacting them.	Mobile-app of Facebook used to entice children to produce images and extort them in an ongoing manner	Mobile-app of social media used variably to 1) transmit child pornography and deceive of online fake identity, 2) procure child pornography, 3) conduct extortion	As part of the scheme, Bivins-Breeden contacted the victims via Facebook on his iPhone posing as a juvenile female and enticed them to produce child pornography. After the juvenile victims produced the pornographic images, they sent them to Bivins-Breeden over the Internet. When the victims refused to produce additional child pornography images, Bivins-Breeden threatened to send the previously obtained images to the victims' friends, family, and schoolmates on Facebook
KANSAS CITY, MO—Tammy Dickinson, United States Attorney for the Western District of Missouri, announced today that a Tennessee man who is a registered sex offender has been sentenced in federal court for using the Internet and a cell phone to attempt to entice a minor to engage in sexual activity. John Richard Fortenberry, Jr., 38, of Murfreesboro, Tennessee, was sentenced by U.S. District Judge Greg Kays on Wednesday, April 9, 2014, to 27 years in federal prison without parole. Fortenberry, who pleaded guilty on November 26, 2013, was a registered sex offender in Tennessee at the time of the offense. He was previously convicted of indecent liberties with a child. In January 2013, an acquaintance of Fortenberry contacted the FBI to report that he was in contact via Facebook with a 12-year-old girl in the Kansas City, Missouri area. Their Facebook messages indicated that Fortenberry was planning to travel to Kansas City to meet the victim in person and engage in sexual activity. According to court documents, the federal investigation established that Fortenberry had been in constant and continual contact with the minor victim via Skype, Facebook, e-mail, and phone since she was 11 years old. Fortenberry and the minor victim would mutually masturbate and watch pornography together while talking on Skype. FBI agents found approximately 1,200 text messages between Fortenberry and the minor victim, dating back to November 2012, on the victim's cell phone. Agents also discovered a video of Fortenberry masturbating and nude photographs of the victim on the cell phone. Fortenberry was controlling, threatening, and coerced the minor victim, according to court documents. The minor victim stated that Fortenberry, who had access to her Facebook account, deleted any of her friends whom he thought were a "threat." The minor victim also reported that Fortenberry controlled her activity on Facebook and threatened her to the point that she was scared. He threatened to commit suicide if the minor victim did not follow his orders to reformat her computer in order to hide evidence from law enforcement. After Fortenberry became aware of the investigation, he not only coerced the victim into reformatting her computer, but he reformatted his own hard drive to hide evidence of the crime. After Fortenberry was arrested and incarcerated he made numerous attempts to contact the victim. According to court documents, law enforcement officers obtained letters from Fortenberry's mother that were written and sent to her by Fortenberry. In these letters, he instructed his mother to communicate with the minor victim on his behalf and asked his mother to send him photographs of the victim. This case was prosecuted by Assistant U.S. Attorney Teresa Moore. It was investigated by the FBI and the Lee County, North Carolina Sheriff's Department.	1) No identiy masking for the production of imagery 2) Real-time online exposure of imagery/video 3) 1,200 text messages uncovered including evidence of photographs/videos	Skype, Facebook, e-mail and phone use	Teleconferencing used for real-time online exploitation. Account take over (ATO) of Facebook with extortion/threatening behaviour associated with it. An incredible persistance developed over 1,200 text messages.	The offender has been in constant use with the 11 year old victim over a number of online channels and over the phone. As young users, children can become really vulnerable over prolonged periods. Time is critical here. Also, younger children could succumb to ATO-threats

FBI case description on release	Image use/distribution	Social network (or other channel)	How criminals used technology	Description and user implications
FRESNO, CA—A federal grand jury returned a two-count indictment today against Brian Caputo, 25, of Arvin, charging him with sexual exploitation of a minor and receipt and distribution of child pornography, United States Attorney Benjamin B. Wagner announced. According to court documents, Caputo for the past eight years has used social media accounts with Facebook, Kik Messenger, and Text Me!, as well as Yahoo! and Dropbox accounts to communicate with dozens of minor females throughout the United States while posing as a minor female. Soon after establishing communication with the minor females, Caputo would threaten to reveal sexually explicit images of their friends unless the minor females created and sent to him images of themselves nude or engaging in sexually explicit conduct. In June 2013, Caputo contacted a 12-year-old girl in El Paso, Texas, and threatened to distribute sexually explicit pictures of her 11-year-old friend unless she sent nude images of herself to Caputo. She told a family member who contacted the El Paso Police Department, and they started an investigation. When law enforcement investigators traced the threatening communications to Caputo, they discovered that he had been victimizing many other minor females across the United States. For example, Caputo convinced one minor female to take and then upload more than 660 sexually explicit images of herself to a Dropbox account controlled by Caputo. When agents executed a search warrant at his residence in Arvin on February 28, 2014, Caputo's cell phone contained hundreds of images of girls ages 11-15 undressing, nude, or engaging in sexually explicit conduct. **Caputo then traded the images with other Internet users.** To date, at least eight minor females have been identified, although law enforcement is attempting to confirm the identity of many other victims. Caputo established Facebook accounts and contacted minor females using the names Giavanna Derann, Catness Love, Melissa Harpson, Cristal Dafnie, and Britt Any. Anyone who believes that they might have been a victim of Caputo's offenses is encouraged to contact the FBI's Bakersfield Resident Agency at (661) 323-9665. Brian Caputo, 27, pleaded guilty to receipt and distribution of child pornography on May 16, 2016. U.S. District Court Judge Lawrence J. O'Neill of the Eastern District of California sentenced Caputo and also ordered him to serve 15 years of supervised release.	1) Imagery was both received/distributed 2) 1 victim (one minor female) uploaded 660 explicit images to an offender-controlled Dropbox account 3) The offender traded the images with other internet users. 4) Multiple images/established identities	Facebook, Kik Messanger, Text Me!, Yahoo!, Dropbox	Cloud-based storage used by offenders for receiving imagery, along with several social media accounts for establishing communication with minors.	Offender convinced one minor female to take and then upload more than 660 sexually explicit images of herself to a Dropbox account controlled by the offender. This raises a clear issue of a disproportional rate of images that can be generated by one 'compliant' and intimated victim. Underground market flooding can occur in this regard. Users that find themselves in the position of a compliant victim may generate a lot of imagery for offenders that use them for trading or other purposes.

APPENDIX 4 – Time slices during Phase 1



APPENDIX 5 – Grounded theory approach (adapted by Charmaz, 2014)



A diagram of our approach in the grounded theory process (adapted based on Charmaz (2014))

Dionysios S. Demetis is an associate professor (senior lecturer) in management systems at the Hull University Business School. He holds a PhD on anti–money laundering and information systems from the London School of Economics and his research concentrates around systems theory, anti-money laundering and cybersecurity. He is the author of two books, one on the philosophy of science and the intrinsic paradoxes of knowledge creation (entitled *Science's First Mistake: Delusions in Pursuit of Theory,* published by Bloomsbury), and another on the systems theoretical deconstruction of Anti-Money Laundering and the role of information systems in it (entitled *Technology and Anti-Money Laundering: a systems theory and risk-based approach,* published by Edward Elgar). He has authored numerous other publications, and his research on anti–money laundering has been featured in the United Nations bibliography and has been funded by the European Commission. He is a co-chair of the International Security Conference in Las Vegas, NV, and a Senior Editor at the Journal of Information Systems Security.

Jan Kietzmann is a professor of Management Information Systems at the Gustavson School of Business at the University of Victoria (Canada). The focus of Jan's work is on organizational and social perspectives related to emerging technologies, with particular emphasis on the intersection of technology and marketing. Currently, Jan works on research on "the Dark Side of Social Media", "Deepfakes", and generally speaking, how Artificial Intelligence and Machine Learning impact firms. Jan's work has been accepted for publication in *Journal of Advertising Research*, *Industrial Marketing Management, MIS Quarterly Executive* and *California Management Review*, among other journals. Jan is probably best-known for his award-winning article "Social media? Get serious!" in Business Horizons, where he now also serves as an Associate Editor.