

## Exploring the police response to technology-driven changes in online child sexual exploitation offending.

# Submitted to The University of Nottingham for the Degree of Doctor of Philosophy, March 2024. Michael Harmson-Silvestri, MSc, BSc. 2019764

Supervised by

First Supervisor:

Professor Chris Greenhalgh,

The School of Computer Science, The University of Nottingham.

Second Supervisor:

Dr Melanie Jordan,

The School of Sociology and Social Policy, The University of Nottingham.

Signature. M Harmson-Silvestri

Date. 03/04/2024

#### **Abstract**

This thesis explores the digital and social media knowledge and training of police officers who investigate online Child Sexual Exploitation Material (CSEM) offending. The training and digital and social media knowledge of those who work within online sexual crime investigation have been largely overlooked. When exploring online CSEM offending, current and existing literature has often focused on police cybercrime investigation overall, including fraud, harassment and stalking. Appropriately, this thesis attempts to fill some of the gaps in the knowledge regarding police training related to online CSEM investigation and recommendations for future policy and practice.

The study employs a constructionist ontological position and an interpretivist epistemology using a convergent mixed-method approach. The study involves two stages. Stage one of this study is comprised of semi-structured interviews with front-line police officers and civilian staff working within online sexual crimes investigation. In total, 11 participants were interviewed. Data were collected and then transcribed using approved university transcription software. The data were then coded and analysed using a process of thematic analysis. During stage two, quantitative data were explored using existing data from the Internet Watch Foundation. The data were coded and analysed using a thematic analysis of specific themes related to online CSEM offending and the risk to children.

The resultant findings suggest that the training and knowledge of police officers working in online sexual crime investigations are inconsistent with the serious nature of their roles and responsibilities. Other findings suggest that there is a need for police leadership to adopt learning theories to enable policing organisations to retain and share knowledge with academics and practitioners on new offending behaviours identified. Additionally, there is a need for formal accreditation for officers working in online CSEM investigations and a consistent approach to their training and knowledge sharing. Officers working in online CSEM investigation also have a responsibility to engage in self-directed learning and continuing personal development regarding new knowledge related to the changing nature of social media and the digital platforms used for online CSEM offending.

Regarding the data analysis from the Internet Watch Foundation. Findings suggest that online technology companies are now the primary responders to online CSEM offending, much younger children than previously known are at risk of sharing self-generated image content, and more children from Western backgrounds are at an increased risk of online live-stream sexual abuse. Finally, online CSEM offenders are now offending across several spectrums of child sexual abuse, including, sexualised grooming, possession of indecent images, physical contact offending and online sexualised chat.

Keywords: Online sexual offending, online CSEM offending, police training, cybercrime, digital knowledge, social media, technology, self-generated images.

#### Acknowledgements

To begin, I want to thank my supervisors, Prof Chris Greenhalgh and Dr Melanie Jordan for their wisdom, guidance and ongoing support over some difficult periods during the writing of my thesis. I would also like to acknowledge my eternal thanks to the officers and staff of the police service who allowed me to conduct my interviews in difficult circumstances, especially during the COVID-19 pandemic and lockdown. In addition, these officers and staff afforded me their time despite working in an extremely stressful and busy work environment.

I also wish to thank and acknowledge my wife, Yongzhen who has supported me through this long and sometimes stressful process and encouraged me whenever I faltered. Finally, I wish to mention and thank my mother, Michelina Silvestri who is no longer with us. My mum was an immigrant who came to this country and couldn't speak English. She had to leave school at eleven when her mother died and did not have an education, yet she taught herself to speak, read and write English, eventually working in the care system. She taught me so much and encouraged me to be the best person I could be through hard work and education. To this end, I dedicate this work to her.

The Engineering and Physical Sciences Research Council (Grant number EP/S023305/1) supported this work.

## **Table of Contents**

ABSTRACT	2
ACKNOWLEDGEMENTS	4
TABLE OF CONTENTS	5
LIST OF TABLES	10
LIST OF FIGURES	11
ABBREVIATIONS	12
CHAPTER 1. THE INTRODUCTION	14
1.1. The motivation for the study	15
1.2. Reflective thoughts on the motivation for the study	18
1.3. Thesis aims	20
1.4. Thesis structure	21
CHAPTER 2. THE LITERATURE REVIEW: PART ONE	23
2.1. Introduction	23
2.2. The history of cybercrime and online CSEM offending	24
2.3. The criminal exploitation of the internet and social media	26
2.4. The use of technology in the responses to online CSEM offending	30
2.4.1. PhotoDNA and PhotoDNA for Video	31
2.4.2. Child Abuse Image Database (CAID) and other classifiers	33
2.4.3. Web crawlers	35
2.4.4. The online CSEM referral system	36
2.5. Social media, government and technology industries' responses to online CSEM offending a prevention	and 37

2.6. Recommendations for future global responses to detection and prevention technology	40
THE LITERATURE REVIEW: PART 2	42
2.7. Introduction	42
2.8. An overview of police cybercrime investigation	43
2.9. Police training and knowledge related to online CSEM investigations	46
2.10. The police E-Learning training system	48
2.11. Technology adoption models and theories related to police training	50
2.12. Formal accreditation for staff working in CSEM investigations	54
2.13. The risks of newer technology in online CSEM offending	57
2.14. The use of social media and the open web in online offending behaviour	59
2.15. The typologies of online CSEM offenders	62
2.16. Other online cybersex crimes and offending typologies	64
2.17. Conclusion	67
CHAPTER 3. METHODS AND METHODOLOGY	68
CHAPTER 3. METHODS AND METHODOLOGY 3.1. Introduction	68 68
3.1. Introduction	68
3.1. Introduction 3.2. The overarching study question	68 69
3.1. Introduction 3.2. The overarching study question 3.3. An overview of the study methodology	68 69
3.1. Introduction 3.2. The overarching study question 3.3. An overview of the study methodology 3.4. Ontology	68 69 69
3.1. Introduction 3.2. The overarching study question 3.3. An overview of the study methodology 3.4. Ontology 3.5. Epistemology	68 69 69 73
3.1. Introduction 3.2. The overarching study question 3.3. An overview of the study methodology 3.4. Ontology 3.5. Epistemology 3.6. Symbolic interactionism related to constructivism	68 69 73 74
3.1. Introduction 3.2. The overarching study question 3.3. An overview of the study methodology 3.4. Ontology 3.5. Epistemology 3.6. Symbolic interactionism related to constructivism 3.7. Inductive and deductive perspectives	68 69 73 74 76 80
3.1. Introduction 3.2. The overarching study question 3.3. An overview of the study methodology 3.4. Ontology 3.5. Epistemology 3.6. Symbolic interactionism related to constructivism 3.7. Inductive and deductive perspectives 3.8. The case study	68 69 73 74 76 80 83
3.1. Introduction 3.2. The overarching study question 3.3. An overview of the study methodology 3.4. Ontology 3.5. Epistemology 3.6. Symbolic interactionism related to constructivism 3.7. Inductive and deductive perspectives 3.8. The case study 3.9. The study method	68 69 73 74 76

3.13. Ethics and reflexivity	101
3.14. Reflexive practice	107
3.15. Conclusion	108
CHAPTER 4. THE PARTICIPANT INTERVIEWS	110
4.1. Introduction	110
4.2. An overview of the interview questions	111
4.3. The qualifications and training needs related to online CSEM investigations?	116
4.4. Role accreditation and Image grading training	123
4.5. What are the difficulties in image grading training?	127
4.6. What is the current level of training for officers investigating CSEM offending?	131
4.7. Additional training needs for staff	134
4.8. The training and awareness of online digital platforms and social media	138
4.9. The experience of knowledge sharing	146
4.10. What is the impact of police officers' knowledge and changes to online offending behavio	ours? 153
4.11. The use of social media knowledge and awareness during suspect interviews	159
4.12. Conclusion	162
CHAPTER 5. THE INTERNET WATCH FOUNDATION SECONDARY DATA ANALYSIS	167
5.1. Introduction	167
5.2. The history and purpose of the Internet Watch Foundation?	169
5.3. The ages of children identified by the IWF in CSEM	170
5.4. The gender of children identified in online CSEM	174
5.5. The rise in self-generated images of children	181
5.6. The ages of children sharing self-generated images	185
5.7. Younger children sharing self-generated images	189
5.8. The changes in online technology and the risk to children	191
5.9. What technology are children using to share self-generated images?	195

5.10. What social media apps are children using to share self-generated images?	198
5.11. YouTube and the concerns regarding self-generated images	201
5.12. What are the possible causes of the rise of live-streaming online abuse?	203
5.13. Limitations	206
5.14. Conclusion	207
CHAPTER 6. THE DISCUSSION	212
6.1. Introduction	212
6.2. Are policing organisations sufficiently prepared to meet the changing nature of online technology used in CSEM offending?	nol- 213
6.3. New oil? Are technology companies now the primary responders to online CSEM offending	? 221
6.4. How changes in technology have affected the online risks to children	225
6.5. How changes in technology have affected online CSEM offending behaviour	229
6.6. Limitations	231
6.7. Implications for policy and practice	232
CHAPTER 7. THE CONCLUSION	236
7.1. The achievements of the study	236
7.2. Police knowledge and training	237
7.3. Official accreditation for officers	238
7.4. The level of social media knowledge and awareness of police officers and staff	239
7. 5. Retaining and sharing new knowledge of offending behaviours	239
7. 6. Collaborative working experience	241
7. 7. How can police be better trained to investigate online CSEM?	242
7.8 Official accreditation for officers working in online CSEM investigation	243
7. 9. Formal structures for learning and training	243
7. 10. Image grading training	243
7. 11. Retaining and sharing knowledge of new offending behaviours	244
7. 12. Has the evolving nature of online digital technolgy changed offending behaviours?	244

7.13. Have the advances in online technology changed the risk to younger children?	245
7.14. What is the changing role of the technology industries in online CSEM detection and counmeasures?	ter- 246
7. 15. Future outlook and recommendations	248
7.16. Feasibility and timeframe for recommendations	250
7.17. Conclusion	252
WORD COUNT: 95,976	253
REFERENCES.	254
APPENDIX A: FOI REQUEST, THE METROPOLITAN POLICE	320
APPENDIX B: FOI REQUEST, WEST YORKSHIRE POLICE	321
APPENDIX C: FOI REQUEST, WEST MIDLANDS POLICE	322
APPENDIX D: E-MAIL. PERMISSION RESPONSE FOR USE OF DATA, FROM THE INTERNET WATCH FOUNDATION	R- 323

## List of Tables

1.1. Duggan & Brenner (2012) The Landscape of Social Media Users.	P. 15
2.1. McGuire (2019) Cybercrime Terminology Used in Academic Literature.	P. 27
2.2. McGuire (2019) Cybercrime Terminology Used in Academic Literature.	P. 28
2.3. Taylor & Quayle Copine Scale.	P. 33
2.4. Broadhurst (2021) Oliver Scale Classification.	P. 34
2.5. Krone's (2004) Typology of Internet Child Abuse Offenders.	P. 62
3.1. Watkins (2003). Core Mixed Methods and Design Definitions.	P. 71
3.2. Yin (2009). Types of Case Studies Used in the Research Process.	P. 84
3.3. Braun & Clarke (2014). Stages of Coding and Analysing Data.	P. 97
4.1. Leading Social Media Apps Globally in 2022 (Kemp, 2022).	P. 144
5.1. IWF Primary Data Sets Analyised-2009-2021.	P. 167
5.2. Ages of Victims Identified in Online CSEM-2009-2016 (IWF, 2021).	P. 171
5.3. Ages of Victims Identified in Online CSEM-2017-2021 (IWF, 2021).	P. 172
5.4. Age Preference Labels Derived From Greek Roots (Sato, 2017).	P. 173
5.5. Data from Thorn Report (2022).	P. 198
5.6. Digital Sites Most Abused for Hosting CSEM (IWF, 2021).	P. 199
6.1. Typologies of Complex Online CSEM Offenders.	P. 216

## List of Figures

3.1. Bryman (2004). The Process of Deduction.	P. 80
3.2. Watkins (2023). Convergent Design With New or Secondary Data.	P. 90
3.3. Bhutta (2004). Conceptual Framework.	P. 104
4.1. Argote & Miriam-Spektor (2010). Theoretical Framework for Analysing	
Organisational Learning.	P. 147
4.2. The SCEI Model. Nokaka & Takeuchi (1995).	P. 151
5.1. IWF (2020). Self-Generated CSEM Abuse-11-13 Years Old.	P. 174
5.2. IWF (2020). 7-10-Year-Olds, Type of Abuse.	P. 177
5.3. IWF (2022). Age Comparison in CSEM Over the Past Three Years.	P. 178
5.4. IWF Data, Percentage of Female Gender Located in CSEM -2011-2021.	P. 178
5.5. IWF Data, Percentage of Male Gender Located in CSEM-2011-202.	P. 186
5.6. IWF Data, Severity of Analysis of Category of CSEM Affecting Boys-2021.	P. 193
6.1. The Department for Education (DOE) RSE Guidance Document (2022).	P. 233

#### **Abbreviations**

CSEM Child Sexual Exploitation Material

ABE Achieving Best Evidence

AI Artificial Intelligence

CAID Child Abuse Image Database

CEOP Child Exploitation and Online Protection Centre

CGI Computer-Generated Image

CID Criminal Investigation Department

CNN Convolutional Neural Networks

CPD Continuing Personal Development

CSA Child Sexual Abuse

CSAE Child Sexual Abuse and Exploitation

CSE Child Sexual Exploitation

DHEP Detective Degree Holder Entry Programme

EBP Evidence-Based Policing

FOI Freedom of Information

HMIC His Majesties Inspectorate of Constabulary

ICIDP Initial Crime Investigators Programme

IIOC Indecent Images of Children

IICSA Independent Inquiry into Child Sexual Abuse

IoT Internet of Things

IWF Internet Watch Foundation

NCA National Crime Agency

NCALT National Centre for Applied Learning Technologies

NGO Non-Government Organisation

NMEC National Centre for Missing and Exploited Children

NSPCC National Society for the Prevention of Cruelty to Children

MFM Motivational Facilitation Model

OFCOM Office of Communications

PIP Professional Investigation Programme

ROCU Regional and Organised Crime Unit

SCAIDP Specialist Child Abuse Investigators Development Programme

SDA Secondary Data Analysis

SGI Self-Generated Images

SSI Social Science Interview

TA Thematic Analysis

TAM Technology Adoption Model

UCO's Undercover Officers

URL Universal/Uniform Resource Locator

VSP Video Sharing Platform

VR Virtual Reality

'The continuing evolution of human behaviour as a result of technological innovations has created unparalleled opportunities for crime and misuse.'

(Holt et al., p.5)

#### Chapter 1. The Introduction

This study explores what is currently known about the digital knowledge, training, and social media awareness of police officers in England and Wales who investigate online child sexual exploitation material offending (CSEM). The study also explores how changes in technology are affecting the policing of online sexual crimes investigation and what can be done to improve the training of police officers, their working practice and organisational regulation. In addition, the online risks to children are addressed related to changes in the age demographics of those most at risk, the rise in self-generated images of younger children and the contribution from the technology industries in combatting online CSEM offending and changes in online CSEM offending behaviour.

This study involves a qualitative investigation using semi-structured interviews (n-11) of police officers and staff in a large English police force working in front-line CSEM investigations. Also, the study uses existing data from the Internet Watch Foundation to explore the changing trends in online CSEM offending behaviour, emerging risks to children related to age, gender and their use of social media and technology. Together, the study will attempt to answer the specific research question: Are police officers keeping pace with technology-driven changes in online child sexual exploitation offending? While this question is the primary research focus, it is underpinned by other sub-questions relating to how technology changes affect online CSEM offending and the risk to children.

Duly, the other sub-questions ask: How can police officers be better trained to investigate online sexual crime offences against children? Has the evolving nature of digital technology changed offending behaviour and the police responses to online sexual crimes? The remaining questions ask, are the advances in online technology changing the risk to younger children, and what is the changing role of the technology industries in online child sexual exploitation detection and countermeasures?

To acquaint the reader with an overview and background of online CSEM offending and the policing response, the introductory chapter will also include two sub-sections which will introduce the reader to the following subjects, a brief history and construct of the UK police service and the law and legislation relating to online sexual crimes. These topics have been included in the introduction as they provide the reader with some background material to support what will come in the subsequent chapters. To begin, an overview of the thesis aims, structure and motivation is provided to guide the reader as to the foundations of this work.

#### 1.1. The motivation for the study

Traditionally, police officers who investigate online CSEM offending are police detectives, suitably trained civilian investigators, or, more recently, direct entrant detectives. Generally, 'medium level' online sexual offences are investigated by detectives within traditional Criminal Investigation Departments (CID). Despite this, serious or 'high-level' online sexual offending is dealt with by specialised online sexual crime units. These units are not to be confused with undercover officers deployed on live peer-to-peer chat sites within Regional Organised Crime Units (ROCUs) or officers in the National Crime Agency.

As a former police officer working in online CSEM investigations, the researcher wanted to discover if the criteria and online knowledge and awareness had changed for police officers working in this field from when they had last worked in this environment from 2012-2015. Previously when working in child safeguarding and online sexual crimes investigation, the author had no formal training regarding social media knowledge or the digital platforms used by offenders. Indeed, the only qualifications required to work in this field were having substantive detective status and completing the College of Policing, Specialist Child Abuse Development Programme (SCAIDP)

If we are to make comparisons related to online child sexual exploitation offending in 2012 when the author first entered this role it is important to gain some context as to how offending behaviour looked like then. For example, the internet and social media use although well established in 2012 was much different to what we know today. Illustrating this, Duggan & Brenner (2013) highlight the main social media platforms in 2012 as seen in Table 1.1.

Table 1.1. Duggan & Brenner (2012) The Landscape of Social Media Users

Social Network Site	% of Internet Users	
Facebook	67 %	
Twitter	16 %	
Pinterest	15 %	
Instagram	13%	
Tumblr	6%	

As noted in Table 1.1., (Duggan & Brenner, 2013), in 2012, Facebook was the most popular social media platform, followed by Twitter. Compared to today, social media platforms such as YouTube and TikTok are now considered the most popular social media platforms, particularly among children and young people (Anderson et al., 2022). However, today, according to Kemp (2022), globally, WhatsApp and Instagram are the leading social media platforms for the 16 to 64 age demographic.

Yet, despite the popularity of some social media apps and the passage of time, social media platforms remain as popular today as they were in 2012. To place this into context, today, there are 7.9 billion people across the world, with 4.62 billion social media users with an average use of 2.5 hours each day (Global Overview Report, 2022). Taking this into consideration, law enforcement agencies a faced with a massive task in trying to police this phenomenon. Ergo, police officers and the police service face several challenges in investigating and identifying online CSEM offenders due to the massive scale of recurring offences (Bursztein et al., 2019)

Other differences are noted from online CSEM offending in 2012 when compared with today, such as offending behaviours and the countermeasures used by criminal justice agencies to detect the offenders. For example, earlier work by Wolak et al. (2012) suggests that at the time, most online CSEM offenders were usually convicted of downloading child abuse imagery and were easily detected by law enforcement agencies as the perpetrators used credit cards to purchase child abuse material. Illustrating this, Metcalf (2007) describes how in 2002, the American FBI (Federal Bureau of Investigation) passed on details of 7,272 individuals to UK police forces who had downloaded indecent images of children, paid for by credit cards.

By comparison, online CSEM offending today has become more sophisticated with offenders using an array of new and emerging technology including social media (Finklehor et al., 2022). Moreover, smartphone technology has developed at a fast rate compared to mobile telephones in 2012, where users had access to a limited amount of applications and most did not allow 'Facetime' video calls such as WhatsApp, and Messenger. However, despite the changes in technology used in online CSEM offending, the main response to this concern by police forces across England and Wales was and is the use of specialised police units. Yet, the argument contained in this thesis suggests that in terms of training and knowledge of police officers in the area of social media and technology related to online CSEM offending, little has changed.

Having joined the police service, investigating everyday crimes such as theft and assaults, is usually carried out by frontline uniform response officers. Those wishing to join specialised police units usually require formal detective training.

Once officers have completed their training, the detectives are placed in various departments, including CID, safeguarding, domestic abuse and counterterrorism. After completing their training, detectives can apply for specialised roles such as online sexual crime units in their respective forces. Applying for roles within online sexual crimes units typically involves an application process followed by a formal interview. Once officers and staff are in their roles working in CSEM investigations, it is prudent to ask what level of training and digital and social media knowledge these individuals possess to enable them to work effectively in this environment.

## 1.2. Reflective thoughts on the motivation for the study

Reflexivity is covered in some detail in Chapter 3, the Methods and Methodology, however, reflexivity is an important contribution to the motivation for this thesis and the overall study. As Kinitz (2022) posits, research involving some personal relevance to the researcher requires a tangible degree of reflexivity which is centred on the research and how the research impacts them. As a former police officer, the area of online CSEM investigation resonates and is an important part of who the researcher is, their motivation, ideas and reflective practice, where knowledge can be gained and used effectively in improving service delivery. Illustrating this, when the researcher last worked in this type of policing environment in 2015, any knowledge of social media or online digital platforms was self-taught and not a requirement for the role. As such, the only requirement for working in child abuse enquiries and online CSEM investigation was being a substantive detective and in some cases, having image grading training.

During this time, the author investigated many offences involving child sexual abuse, including online sexual crimes which usually involved image-based offences and sexual grooming of children. However, despite the serious nature of the role, the author felt some concerns regarding their ability and confidence to investigate these crimes effectively without the correct training and knowledge of social media and the digital platforms used in online CSEM offending. Consequently, the author continued on a predictable path of receiving referrals, arresting the suspect, having their devices forensically examined by a hi-tech crime unit and then reading out the forensic report to the suspect during the police interview.

Subsequently, the author gained minimal knowledge of how the suspect had accessed the child abuse images and why they had chosen a particular digital platform.

Having retired from the police service in 2015, the author then embarked on a Master's programme and then briefly in the sex offender management unit, of a large English police force, assessing the risk of convicted sex offenders who were placed on the national sex offender register. The author noted that the offenders had been convicted of physical sex offences but also online CSEM offences. Indeed, several had been convicted of sexual activity with a child and also possession of indecent images and sexualised grooming.

After speaking to the offenders, the author gained some insight into how they engaged with the child victims online and also how they accessed and shared child abuse material with others. How offenders accessed online CSEM sparked an interest in the author as much of the previous literature on online child sexual offenders had focused on typologies of offenders and behaviours (Tenner et al., 2015; Paquette et al., 2020).

During this period, the author commenced this thesis, initially exploring the theories of what technology online CSEM offenders were using to sexually groom and exploit children. To gain more insight into the phenomenon of online CSEM offending, in 2019, the author began a volunteer placement within the online sexual crimes unit in a large police force in England. It was during this stage that the author gained some anecdotal and first-hand evidence related to the training and knowledge of the officers and staff working in this unit.

At this time, the author witnessed how the dedicated officers and staff in this unit worked in such a serious environment without being afforded the requisite training, accreditation and knowledge worthy of their role. Resultantly, the ideas and motivations for this thesis were developed during this period where the research questions were formulated. The questions developed by the researcher related to the research area illuminated what the researcher saw as a valid and important discussion regarding how the modern police service is prepared to effectively tackle the problem of online child sexual exploitation offending. Due to this, the research process began with a qualitative investigation with those who work first-hand in such a difficult and emotive area.

The police officers and civilian investigators in this study form the backbone of the overall research as they are the ones who investigate some of the most serious crimes against children. Given the enormity of their task, it is fitting that the officers and staff in these units are suitably trained for such a challenging task. Is being a detective and holding image grading training enough to warrant entry into online sexual crime units without any additional knowledge or training? Is it acceptable in such a specialised and sensitive role that there are differences across other police forces in training and knowledge? These questions are valid, and as a result, this thesis argues that these issues have been previously overlooked in academic literature. Therefore, the motivation for this study is laid out by the researcher.

#### 1.3. Thesis aims

Following on from the motivation for this study, the aims of the thesis are now outlined. This thesis aims to broaden our understanding and knowledge of what is known about digital and social media, awareness and training of police officers investigating online Child Sexual Exploitation Material offending (CSEM). In addition, this thesis aims to explore the changing nature of online CSEM-offending technology related to the new and emerging risks to children. Moreover, this work also aims to explore the technology industries' contribution to online CSEM countermeasures as the primary responders to this phenomenon. Hence, these areas deserve further attention as most existing studies in this field have focused on general policing responses to cybercrime overall, such as theft, hacking and fraud.

For the qualitative aspect of this study, the participants share a common trait: they are part of a police organisation that due to the findings in this study may differ in some way from other policing regions and areas in the investigation of online sexual crime. As such, the differences in police officers' training and knowledge in online CSEM investigation is an area of interest which deserves further investigation.

The unit where the participants in this study worked was relatively small, incorporating approximately 14 officers and staff with varying ages and levels of online technical knowledge and social media awareness. To this end, the study aimed to assess the online knowledge and training of these officers compared to other similar police units.

On this account, research proposals were submitted to other police forces, criminal justice agencies, charities and the National Crime Agency to try and answer this question, however, these proposals did not come to fruition for several reasons which will be explained in Chapter 7, the conclusion.

In response to this barrier, this thesis has used Freedom of Information Requests Appendices (A, B and C) from three other large UK police forces to gain some context as to how other officers and staff are trained in online CSEM investigations. This subject will be covered more in-depth in subsequent chapters. Accordingly, exploring these areas is an important consideration for policing organisations and academia which will help to increase knowledge related to the fluid and changing nature of online CSEM offending including the online technology industries' responses.

#### 1.4. Thesis structure

The thesis is comprised of seven chapters. Chapter 1 is a prologue to the work and introduces the reader to the study's research question, aims and motivation. In addition, this chapter provides valuable background information for the reader to acquaint themselves with the phenomenon of online child sexual abuse. Chapter 2, the literature review, will focus on relevant literature regarding police cybercrime, police cybercrime training, typologies of offenders, the technology industries' responses to online CSEM, countermeasures and the changes in the online risk to children.

Chapter 3 incorporates the methods, methodology, epistemology, ontology, and methods applied to the research conducted. Chapters 4 and 5 focus on the participant interviews and secondary data analysis using Internet Watch Foundation data. Chapter 6 will discuss the findings of the research and implications, while Chapter 7 summarizes the overall study and suggests recommendations for future research, policy, and practice and how they can be achieved.

The next main chapter is Chapter 2, the literature review. As the literature in the area of online CSEM offending and cybercrime and technology is vast, Chapter 2 is divided into two parts. Part one will review the literature on cybercrime, its history and cybercrime offences.

Part two of the literature review will focus on child sexual exploitation material offending, police training and responses, the typology of online CSEM offenders and the technological countermeasures used to identify and remove online CSEM material.

'Historically speaking, the problem of child sexual abuse has been grossly neglected. "it is only in relatively recent times that the nature and scale of the problem have come to be publicly acknowledged and politically addressed.'

(Yar & Steimetz, 2019, p.180)

## Chapter 2. The Literature Review: Part One

#### 2.1. Introduction

As the literature in the area of cybercrime and online child sexual exploitation offending (CSEM) is vast and dates back many years, the literature review in this chapter is divided into two parts. By dividing the literature review into two sections, this chapter will provide the reader with a concise perspective on cybercrime offending, the policing responses, the level of training and the use of technology and the technological responses and countermeasures to online CSEM offending. It is also useful at this stage to revisit the primary research question: Are police keeping pace with technology-driven changes in online child sexual exploitation material offending? As such, the review will address this question by exploring the literature surrounding and addressing the following main headings in order of hierarchy:

- The history of cybercrime and CSEM offending,
- The criminal exploitation of the internet
- The use of technology in the response to online CSEM offending,
- Social media, government and the technology industries' responses to online CSEM offending and prevention,
- Recommendations for future global responses to detection and prevention technolgy.

#### 2.2. The history of cybercrime and online CSEM offending

Mentioning the history of online child sexual exploitation offending and cybercrime is essential if we are to address the initial research question, which asks, 'Are police keeping pace with technology-driven changes in online child sexual exploitation offending? For example, Holt & Bossler (2016, p.1) claim that "cybercrime is a complex and diverse problem, though the nature of studies and methods makes it difficult to assess the totality of the field." Similarly, Holt et al. (2022) argue that over previous decades, there has been a substantial rise in the use of technology by criminals and unique applications of technology to create new forms of criminal offending that previously did not exist.

If we explore the development of online crime, this phenomenon may have been ongoing since the first use of commercial computers. At the time, most of society did not view it as a significant concern and had no reason to suspect that future technology would become so advanced to allow an individual to take an intimate image of themselves and then share it with others on a mass online communication network (Li, 2017). Because of this aspect, improvements in video streaming and smartphone technology have afforded new opportunities for the production and distribution of CSEM material (McCallister, 2014).

The first documented online or computer crime occurred in 1958 when staff fraudulently altered bank records for financial gain (Parker, 1989). Yet, in these early days of computer-generated crime, there were no laws or legislation to combat the slow burn of the evolution of computer crime (Chen, 1990). By the late 1970s, Becquai (1979) placed cybercrime into five categories: vandalism, theft of information, theft of services, theft of property and fraud. Noteworthily, CSEM offending is missing from these categories, suggesting that, Becquai (1979) could not have envisaged how the ease of device use, and the rise of the internet would affect the change in sexual offending behaviour.

Before the internet's development, accessing indecent images usually involved books, VHS video cassettes, polaroid photographs and magazines. In the UK, the Obscene Publications Act 1959 was the primary legislation against those found possessing indent material; however, it was up to the courts to decide what was considered 'obscene.'

For example, the legislation states, "An article shall be deemed to be obscene if its effect or (where the article comprises two or more distinct items) the impact of any one of its items is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it. To deprave means to "make morally bad, to pervert, to debase or to corrupt morally". To corrupt means to "render morally unsound or rotten, to destroy the moral purity or chastity, to pervert or ruin good quality, to debase, to defile." (Legislation. Gov, Obscene Publications Act).

As one can see, the legal definition relating to obscene publications was open to interpretation by the courts. Illustrating this, at the time, some naturist magazines depicting images of naked children were not considered illegal. Today, in the UK, naturist-type images of children could be regarded as class C images in the three categories of indecent images (Sexual Offences Act, 2003). But then, by the early 1990s, home computers could offer individuals access to innovative communication and information which could be used for nefarious reasons. For instance, an early form of sexual contact involved bulletin boards and subscription services. The bulletin boards provided deviant content and information for individuals to contact like-minded others with the same sexual interest and provided quick and widespread contact across the globe with similar deviancy (Durkin & Bryant, 1995).

As early as the late 1980s, law enforcement agencies in the US were investigating child sexual exploitation on bulletin boards, which involved the planned abduction, rape and murder of a 12-year-old boy (Jackson, 1989). Resultantly, the rise in the use of bulletin boards and chat rooms by sex offenders to target children was becoming a significant concern with law enforcement agencies that required adequate training and awareness to tackle the problem (Davis et al., 1995). As one can see, this milestone within internet history is a significant moment that suggests the beginning of online sexual offending behaviour.

By this point, not only were children actively targeted on these bulletin boards by sex offenders, but some minors were also inadvertently engaging with bulletin boards, unaware of their content. Schwartz (1993) provides an account of an eight-year-old girl who inadvertently communicated with a bulletin board and attempted to chat with a group of cross-dressers when she found a site for TVs, with TV being slang at the time for transvestites. The news media reported that the child was trying to chat and make friends and discovered a 'TV Chat' site which she thought was about television programmes. Accordingly, the evidence suggests that despite this primitive technology, at the time, children were at risk of being exposed to sexualised adult content.

Unsurprisingly, children being unsupervised online is not a novel concept but has been ongoing for decades. In earlier literature, Durkin (1997) highlights the concerns of children being unsupervised online by "educating parents" about online safety and "closely monitoring the computer activity of their children." Yet, when Durkin (1997) made these claims, smartphones and tablet technology were unavailable. During the early 1990s, home computers were often large, cumbersome items usually occupying a shared space within the family home. Consequently, it was much more accessible for parents to monitor their children's online use than today, with children having access to the internet on smartphones in the privacy of their room, away from parental intervention. Nevertheless, despite Durkin's (1997) concerns, today, children are still being targeted online more or less in the same way by sex offenders for numerous purposes (Yar & Steinmetz, 2019; Holt et al., 2022; Gillespie, 2019).

### 2.3. The criminal exploitation of the internet and social media

Throughout history, like any other technological developments, the internet and social media have been no different from exploitation by criminals. Evidencing this, Naylor (2004) noted that modern communication technology had some equivalent in the telegraph age, which saw financial fraud conducted by telegraph and wire. Meanwhile, telegraph companies were susceptible to security breaches by hackers, particularly money transfers. As such, the exploitation of technology is not a modern concept and has long been used for financial gain or 'criminal entrepreneurship.'

Criminal entrepreneurship occurs when there is a need for a particular demand for a legal or illicit product (D'ecary-Hetu, 2020). For example, the online distribution and selling of illegal drugs were once commonplace, yet in the early stages, it was easy for law enforcement agencies to identify and take down these unlawful online sites (Henney et al., 1999) In addition, the launch of Silk Road (SR1), an illegal online marketplace or crypto-market, enabled vendors to establish online shops with the look and feel of legitimate online businesses such as eBay (Martin, 2014). Taking this into consideration, it could be argued that during the early days of the Internet, it was open to exploitation by criminals for financial gain.

Crypto markets have grown over the years, earning millions in revenue and other vendors have launched illicit websites on the Tor networks, unlike crypto markets, which are run by one administrator (Kruithof et al., 2016; Yannikos, Shafer & Steinbach, 2018). Moreover, crypto markets using anonymised software allow communication to purchase products online, which can be delivered by traditional postal services (Tzanetakis, 2018). As a result of this criminal exploitation, the UK Home Office spent £1.9 million trying to stop the sale of illegal drugs via the Internet by using recent technology and increasing intelligence on criminal gangs operating online (BBC News, 2017).

Despite the long history of illegal online activity by criminals, including online sales of illegal drugs, many academics have differing opinions on the term used to describe this behaviour. Many scholars and professionals within law enforcement prefer 'cybercrime' to describe online criminal behaviour. Wall (1998) first used the term 'cybercrime' to describe crimes committed or facilitated online. Yet, there is some debate about the differences between cybercrime and computer-assisted crimes. This being so, 'cybercrime' relates to crimes in which the offender has used specialised knowledge of cyberspace, while 'computer crimes' are facilitated by the offender's technical understanding of computer technology (Furnell, 2002; Wall, 2001).

In the days before the internet, Parker (1976) referred to the misuse of information technology as 'computer crime', however, this term soon became outdated with the development of the internet (McGuire, 2019). Moreover, McGuire (2019), Table 2.1. and 2.2., provide extensive use of terminology found in academic literature to define online offending throughout the decades. It is unsurprising that before 2001, the term 'computer crime' was the most used word to describe crimes committed by computer technology. Table 2.1., (McGuire, 2019) illustrates the change in terminology as technology evolved and the internet became more commercialised.

Table 2.1. McGuire (2019). Cybercrime Terminology Used in Academic Literature: 1995-2004

Occurrence
2,750
1,476
585
236
50
49
43
19
17

Table 2. 2. McGuire (2019). Cybercrime Terminology Used in Academic Literature: 2001-2018

Name	Occurrences
Cybercrime or Cyber-crime	28, 100+ 17,900 = 46,000
Computer Crime	19,000
E-Crime	15,800
Internet Crime	7,500
Online Crime	3,830
Virtual Crime	43
Techno-Crime	19
Netcrime	216

When examining the various terminologies used to describe cybercrime offences there appear to be some inconsistencies related to the academic contributions to this field. One such highlighted by Furnell & Dowling (2018) is a lack of agreement with the consistency and categorisation of cybercrime which is a key factor when quantifying similar or related crimes. In addition, Furnell & Dowling (2018) also posit, that although there is an academic discussion related to taking a consistent approach to defining cybercrime and appropriate methods of recording these crimes, how do organisations and criminal justice agencies allocate suitable resources and safeguarding measures given the vast array of definition? Suitably, there is a convincing argument for taking a consistent approach to cybercrime terminology related to the classification and recording of these crimes.

How CSEM offenders use technology to offend is an important aspect of this thesis and relates to what we know regarding the knowledge and training of police officers who work in this environment. Hence, the next section explores how the internet and social media may have influenced online CSEM offending.

After exploring the use of the internet and social media in online CSEM offending, the next main heading explores how the technology industries respond to online CSEM and the countermeasures and detection technology used to identify and remove illegal child abuse images and content. This is an important consideration which is discussed within the literature, suggesting that the online technology industries are now the main responders to online CSEM detection and countermeasures.

#### 2.4. The use of technology in the responses to online CSEM offending

Globally, law enforcement agencies investigate millions of child abuse cases each year, and in 2017, child abuse investigation hotlines received over 37 million child sexual abuse referrals (Pereira et al., 2021). As this global problem increases, technology plays a vital role in identifying and removing online child sexual exploitation material. In response, private companies that manage user-generated data, including Facebook, Microsoft, Apple, and Google, have prioritised detecting and removing child sexual exploitation material from their platforms (Pereira et al., 2021). Accordingly, law enforcement agencies worldwide, including the UK, have deployed technological countermeasures such as the child abuse image database (CAID) (Independent Inquiry Child Sexual Abuse, The Internet, 2020).

The Child Abuse Image Database (CAID) system was initially developed in 2014 to detect CSEM and abuse images by employing PhotoDNA technology, which uses unique identifiers on each image called hash values (Home Office, Child Image Database, 2018). In addition, other global responses exist, including web crawlers such as Canada's Project Arachnid, referral and detection agencies including the US National Centre for Missing and Exploited Children (NCMEC), Project Vic, a Canadian community of investigators and application developers, the UK Internet Watch Foundation and the Five Eyes countries including Australia, US, UK, Canada and New Zealand (Child Dignity Alliance, 2018).

Hence, the global coalition of technology companies suggests that these alliances are now the main responders to online CSEM offending.

The claim that the technology industries are now the main response to online CSME may seem controversial to some, including police and criminal justice agencies. However, to support this argument, it is important to highlight how the technology industries have contributed to the online safety of children by way of online CSEM prevention and detection countermeasures. Thus, the literature explores the technology available to police, criminal justice agencies, government and NGOs in their fight against online CSEM.

#### 2.4.1. PhotoDNA and PhotoDNA for Video

PhotoDNA, used to detect online child abuse images, creates a unique digital fingerprint compared to other images with hashes and can locate copies of the same image (Quayle, 2020). Microsoft first developed PhotoDNA in 2009, and although it relies on hash signatures, it can now compensate for modifications and alterations of images, including reframing, enhancements, colouring and resizing (Guerra, Bryce & Westlake, 2021). In addition, PhotoDNA, when paired with a database containing known illegal child abuse images, can report and disrupt the distribution of online child sexual exploitation material (Steel et al., 2020). On the contrary, a flaw within PhotoDNA relates to the technology identifying known images only. Ergo, as PhotoDNA is a signature-based technology, new or first-generation illegal images cannot be identified and rely on manual identification (Pereira et al., 2021).

PhotoDNA is deployed in many global online companies, including Facebook, Google, and Twitter (Farid, 2018). Like PhotoDNA, PhotoDNA for video is a recent development that uses the same principle for videos and movies. Moreover, "PhotoDNA is used by online service providers and law enforcement agencies who apply the technology to material stored in databases that assist in identifying victims of online sexual abuse" (Broadhurst, 2019, p.315). Nevertheless, a significant flaw within PhotoDNA and PhotoDNA for video is that the technology only effectively recognises and compares identified or known content (Vitorino et al., 2017). In effect, PhotoDNA and PhotoDNA for Video are only as effective as the identified images deployed onto the system.

It is also worth noting that alongside PhotoDNA, private industries have contributed to detection technology by employing commercial software solutions that focus on blocking digital sites. Moreover, the ongoing development of neural networks to identify child abuse imagery ensures that they are classified and taken down much faster (Child Dignity Alliance, 2018). Additionally, significant limitations to Photo and PhotoDNA for video and other detection technology involve a lack of suitable training data (Vitorino et al., 2017; Guerra & Westlake, 2021; Dalins et al., 2018). For this reason, without adequate training data, machine learning cannot evolve quickly enough to identify and recognise known child abuse images.

Also, as PhotoDNA and PhotoDNA for video can only detect previously known images, it is apparent that to detect new images, investigators must rely on content-based methods of detection rather than hash signatures (Vitorino et al., 2017). All the same, finding enough suitable datasets for training is challenging regardless of which technology is available to detect child abuse images (Vitorino et al., 2017). From the beginning of the millennium, online child abuse imagery has been collated and collected by many global law enforcement agencies, charities, and other organisations. Because of this, these images are stored in global and national depositories to detect child abuse victims quickly and shorten the digital forensic examination process (Açar, 2019).

The Child Dignity Alliance (2018) highlights the problem regarding the copious amounts of annotated datasets required by industries to develop tools to train machine intelligence algorithms. Despite this barrier, law enforcement agencies are reluctant to share data due to security, privacy and confidentiality concerns. Moreover, Vitorino et al. (2017) emphasise the problems of detecting child abuse imagery by citing access to relevant data as a concern. On these grounds, one can understand these concerns as any data shared by law enforcement agencies with external organisations could be used for nefarious reasons (Child Dignity Alliance, 2018).

In response to this problem, Açar (2019) calls for a single framework for a global repository for child abuse imagery that an international organisation would govern. While the advantages of a single global repository may increase the efficiency of information and data sharing between stakeholders and law enforcement agencies, this concept represents some significant problems.

Açar (2019) cites many barriers to a shared global repository, including finances, time and resources. In addition, the yearly subscription costs and maintenance alone would be detrimental to less wealthy countries (Açar, 2019). To this end, many countries, including the United Kingdom, may have justifiable reasons for storing known child abuse material, including the CAID database, to prevent them from being used by other countries or individuals for nefarious reasons.

#### 2.4.2. Child Abuse Image Database (CAID) and other classifiers

Currently, all UK police forces now use CAID to identify indecent images on a suspect's device within seconds, saving valuable time and resources, yet as mentioned previously, CAID cannot identify new or 'first-generation images'. Just the same, as with similar datasharing problems. The Internet Watch Foundation, which actively tackles online child sexual abuse in the UK, does not have access to the CAID database. (IICSA, 2020). CAID, alongside PhotoDNA and VideoDNA, scans hard drives for illegal content using various classifiers. In addition, technology industries have also developed similar technology, including deep convolutional networks (CNN), defined as state-of-the-art technology for child abuse image classification (Razavivian et al., 2014; Szegedy et al., 2015). Yet, despite the improvement within this technology, some of these technical solutions rely on skin-based detection, which suffers from false alarms as some adult content could be classed as child abuse material (Vitorino et al., 2017).

The difficulties within skin-based detection technology relate to image classifiers, which often rely on several global classification systems that determine the images' severity. These classifiers include the COPINE scale, the Oliver Scale, and the Interpol International Classification Scheme (Child Dignity Alliance, 2018). Taylor & Quayle's (2001) Copine Scale Table, 2.3., identifies 10 categories of child abuse imagery ranging in severity from 1 to 10. Thus, many technological techniques used within the commercial industry, including classifiers, focus on models that can only detect levels one to three within the COPINE Scale (Vitorino et al., 2017).

More recently, the UK Sentencing Advisory Panel (SAP) reduced the ten categories on the COPINE scale to five as seen in Table 2.4., based on sentencing guidelines often called the 'Oliver Scale' (Broadhurst, 2021, p.315). Other problems affecting the reliability of classifiers and deep convolutional networks (CNN) are based on skin tone, including age and ethnicity. Skin tones, for example, relate to the amount of skin or flesh tone pixels within an image used to gauge the likely probability of nudity (Dalins et al., 2018).

Table 2.3. Taylor and Quayle's COPINE Scale for Sexually Exploitive Imagery of Children

Level of image severity	Description of image
 L1	Indicative (non-erotic pictures)
L2	Nudist (naked or semi-naked in legitimate settings
L3	Erotica (Secretive images showing underwear/nakedness)
L4	Posing (intentional posing suggesting sexual content)
L5	Erotic posing (intentional sexual or provocative posing)
L6	Explicit Erotic Posing (emphasis on genital areas)
L7	Explicit Sexual Activity (sexual activity with no adult involved
L8	Assault (sexual assault involving an adult)
L9	Gross Assault (penetrative assault involving an adult)
L10	Sadistic/Bestiality (imagery involving pain or animals)

Table 2.4. Broadhurst (2021). The Oliver (SAP) Classification

Level of Severity	Description of Image
1	Erotic posing with no sexual activity
2	Sexual activities between children or solo masturbation by a child
3	Non-penetrative sexual activities between children and adults
4	Penetrative sexual activity between children and adults
5	Sadism or bestiality

At the same time, Dalins et al. (2018) argue that skin tone analysis is prone to false results through legitimately exposed skin and unrelated but similarly coloured objects. Because of this, it could be claimed by Dalins et al. (2018) that skin tone classifiers are unreliable disambiguators for identifying child abuse imagery. Further exploration of skin tone analysis can be seen in the work of Russakovsky et al. (2015) and Vitorino et al. (2018).

#### 2.4.3. Web crawlers

Other industry detection technologies include web crawlers designed to collect and classify child abuse material found on public websites (Guerra, Bryce & Westlake, 2021). Web crawlers, called search bots, automatically browse websites and seek out specific data based on pre-selected criteria (Lee et al., 2020). In addition, Web crawlers can also exploit websites for child abuse material by searching for keywords and file names used by online criminal communities (Lee et al., 2020).

Yet, limitations exist in deploying keywords and file name searches as language, terms, and phrases can be altered or become outdated or irrelevant (Guerra, Bryce & Westlake, 2021; Westlake, Bouchard & Frank., 2017; Pereira et al., 2021). Furthermore, offenders are also able to create adversarial inputs that are intentionally created to avoid detection for text applications by substituting text and numbers using "Lo7ita" instead of "Lolita" (Woodbridge et al., 2018). Suitably, the literature on this issue may suggest a need for continued research and development in this area as offenders find new ways of avoiding text detection.

Whilst the review has so far covered countermeasures and detection technology related to online CSEM, it is also important to view the literature regarding how referrals are made to law enforcement agencies and technology providers related to CSEM. Thus, the next section will provide a brief overview of the literature concerning how online CSEM referrals are made by the National Centre for Missing and Exploited Children (NCMEC).

#### 2.4.4. The online CSEM referral system

Turning now to how initial online safeguarding referrals are made; it is essential to understand how they are identified and investigated by criminal justice agencies. Initially, most of the safeguarding responses involving social media and other digital platforms were the responsibility of the National Centre for Missing and Exploited Children (NCMEC). NCMEC, an American-based charity, monitors social media platforms and internet search providers who then refer any suspicious activity, images or search terms to local law enforcement agencies in the country of origin where the offences originated. As a result, NCMEC allocates each complaint of child abuse imagery to the country's law enforcement agencies during the referral procedure, such as the National Crime Agency (NCA) in the UK (NCMEC, 2020).

Analysis of NCMECs (2021) Report by electronic service providers indicates that there were 29,157,083 million reports of child abuse material, up from 21.7 million in 2020. In addition to investigating referrals for downloaded indecent images, NCMEC also refers to what is known as 'self-generated images'. The concern regarding self-generated images is fully discussed in Chapter 5, having said that, it is prudent to give the reader an overview of this phenomenon.

Self-generated images are photos or videos uploaded by a child containing inappropriate or naked images of themselves. For example, Bryce (2010) defines children's self-generated images as 'self-victimisation behaviours' where a child voluntarily engages in sexually-orientated communication. Just the same, it is now accepted that children who share these types of images are often coerced and groomed into providing intimate images and videos of themselves (IWF, 2021).

In trying not to criminalise children, the Internet Watch Foundation (2020) argue that criminal justice agencies should deal with these offences much differently. For this reason, it is essential to understand that children's self-generated images are vastly different from adult-initiated online sexual crimes. Accordingly, to try and quantify the scale of self-generated imagery of children, the UK Safer Internet Centre (UK SIC, 2020) reported that self-generated imagery of children makes up one-third of all sexual abuse material removed from the Internet.

Following this, the Internet Watch Foundation (2021) identified 182,281 URLs that contained self-generated images of children, a 374% increase from pre-pandemic levels. While it is prudent to discuss the technological responses and countermeasures in place by the technology industries to combat online CSEM, there should be some debate on the role and responsibilities of social media companies and government responses when tackling the problem of online CSEM offenders operating on online digital platforms. Therefore, the main section will explore the literature related to this issue.

# 2.5. Social media, government and technology industries' responses to online CSEM offending and prevention

When discussing the role of social media companies and CSEM offending, Gillespie (2018) argues that although social media companies protect users from the online harm they have received, they fail to protect them from exposure. The responsibility of social media companies to adopt a proactive approach to online harm has been an ongoing issue for several years, generating many UK government reports, including the Online Harms White Paper (2019) and now the Online Safety Act (2023).

Initially, the Online Harms White Paper (2019) argued that social media companies' existing regulations and voluntary practices have not gone "far or fast enough" to keep their users and customers safe from online harm. Consequently, The White Paper also called for enforcement and compliance for an independent regulator to oversee the social media companies to ensure they follow procedures and recommendations.

At the time of authoring this thesis, the Online Safety Act (2023) was passed into UK law in October 2023. The Act places a statutory and mandatory responsibility on internet service providers to 'identify, mitigate and manage the risk of harm, including risks which particularly affect individuals with certain characteristics from illegal content that is harmful to children'. Despite this, there is some controversy surrounding this Act related to privacy. For example, the Act will now allow platforms such as WhatsApp to monitor message encryption, meaning that private chats would be checked for illegal content. Hence, there are some concerns related to Ofcom's new wide-ranging powers and challenges to free speech and privacy (Politics, 2023).

Despite some criticisms of the Online Safety Act, many children's charities reacted positively to this new legislation. Before this Act was passed into UK law, the Regulating Online Harms Paper (2021) recommended that social media companies must identify and remove illegal and harmful content, gauge the likelihood of children accessing their platforms and provide additional safeguards and protections. In doing so, this new legislation places even more responsibility on technology companies to design more sophisticated methods regarding the massive task of monitoring private chat messages on all social media platforms.

While it is neither constructive nor correct to place the responsibility of policing online behaviour solely on the technology or social media companies, ideally, there should be a joint strategy amongst criminal justice agencies and social media industries to tackle this problem, but this concept is not new. Earlier work by Wall (2007) called for cooperation between the police and private companies to constitute their role in cybercrime security and prevention. In addition, as far back as the early 21st century, internet service providers who host social media platforms have influenced individuals' online behaviour through contracts, terms, and conditions (Crawford, 2003; & Vincent-Jones, 2000). To this end, users of social media must also have some degree of personal responsibility to adhere to guidelines and personal when using these sites (Merwick et al., 2017).

To further explore the debate on the responsibility of social media use, earlier work by Wall (2007) argued that internet service providers should employ software solutions to reduce online offending with sophisticated spam filters. Given these earlier claims, it is now apparent that most online child sexual exploitation is conducted on the open web, with social media applications such as Instagram and Snapchat being the most common (Davis, 2020; Seigfried-Spellar & Leshney, 2016; Inquiry into Child Sexual Abuse, Learning about Online Sexual Harm, 2019). In addition, one also must consider how the Online Safety Act is going to be policed, given the anticipated rise in online referrals. Considering the vast amount of government policy and attention on this matter, it could be implied that social media companies may not be fully accountable or responsible for their users' online behaviour.

Given this position, it could be argued that future research will be needed to witness the effects of monitoring private chats on social media apps which fall into the criminal offence bracket. Moreover, as the Online Safety Act (2023) places a mandatory duty on companies to remove harmful content, they will also have a duty to report criminal content to law enforcement agencies. More recently, there has been a rise in high-profile criminal cases where whistle-blowers have reported private WhatsApp messages that otherwise would have gone unchecked, which resulted in criminal convictions (BBC News, 2023). In addition, the new Act will now monitor group or private chats on platforms such as WhatsApp for illegal or harmful content. Therefore, it remains to be seen if this new Act will place an even larger burden on already overstretched criminal justice agencies regarding arrests and investigations.

It is envisaged that the Online Safety Act (2023) will impose a regulatory regime preventing illegal and harmful content while placing a duty of care on social media companies and service providers. Yet, critics of the then Online Safety Act argued that in its current form, the wording and legislation were too vague and threatened freedom of speech. In addition, it has been claimed that the Act will place too much control on social media companies and abandon age verification on specific social media sites. Consequently, despite the pros and cons of government intervention in online harm prevention, the evidence suggests that criminal justice agencies, the government, internet service providers, and social media companies should work more collaboratively to reach a mutual purpose (Lepanen, Kiravuo & Kajantie, 2017).

To summarise, the evidence from the literature so far may suggest that the policing of social media when protecting vulnerable children and adults is not the sole responsibility of criminal justice agencies but rather a collective interagency approach involving social media companies, charities, and the police (Holt et al., 2020). At the time of writing, the Online Safety Act (2023) has been enshrined into law, and it is too early to say how this legislation will improve online safety for children, however, it is an ideal opportunity for academics to revisit this area in the future to see what impact this legislation has made on online safety, if any.

To summarise part one of the literature review thus far, the literature has explored the evolution and history of cybercrime, the criminal exploitation of the internet, the rise of the internet and social media and the effects on offending behaviours and the use of technolgy in the response to online CSEM offending. To finish this part of the literature review, the final section will examine the future global responses to online CSEM offending. This inclusion is a vital aspect if society is to collaborate effectively towards the ever-increasing concerns of online CSEM offending.

## 2.6. Recommendations for future global responses to detection and prevention technology

Global responses to the prevention and detection of online child sexual exploitation and abuse deserve attention from both industry and law enforcement (Guerra, Bryce & Westlake, 2021; Lee et al., 2020; Child Dignity Alliance, 2018; Broadhurst, 2021). In addition, the technology industries should work collaboratively to decrease the "fragmented patchwork approaches" to developing prevention and detection technology (Child Dignity Alliance, 2019, p.21). Moreover, law enforcement agencies, including the Five Eyes nations, should encourage a more extensive take-up of high-quality technology. That being so, investing in high-quality technology would encourage multilateral working, ensure greater consistency of working practice, and support the translation of categories within different policing districts (Child Dignity Alliance, 2019).

While prevention and detection technology are essential in combating the rise of online CSEM offending, other methods must not be discounted. For instance, it is suggested that internet and social media companies should invest in more live human moderators and ensure enough are deployed to concentrate on online child sexual abuse and exploitation (IICSA, 2020). Regardless of the use of human moderators, it has its problems. Twitter, for example, does not have enough volunteer moderators and has a poor record when moderating content that is not in English (Euro News, 2023). Somewhat concerningly, it has also been alleged that TikTok human moderators have been exposed to unsecured content of children being sexually exploited as a reference guide (Forbes, 2023).

Hence, social media platforms should look for ways in which AI can support human moderators in a supportive partnership with automated moderation (Gillespie, 2020). Another concern in this area is industries' sharing of technical data and development with law enforcement agencies. The Child Dignity Alliance, Technical Working Group Report (2019) recommended that social media and IT companies such as Facebook, Google, and Microsoft support law enforcement and government agencies by sharing technology to combat online child sexual abuse and exploitation. By that means, law enforcement agencies should focus on the prevention and detection technology of online child sexual abuse and exploitation by treating hashes as a global resource and assisting industries with developing new prevention and detection technology (Child Dignity Alliance, 2018).

Although this section briefly overviews the problem, some solutions may be possible. For example, one answer to this problem lies in the differences in internal laws and policies regarding what constitutes an 'obscene' or a computer-generated indecent image of a child (Yar & Steinmetz, 2019). In addition, many countries have different laws and legislation regarding what constitutes an indecent image of a child and the illegal, moral, and cultural differences in many countries relating to CSEM (Yar & Steinmetz, 2019). For example, what may be considered as child abuse imagery in one country, may not be illegal in another. Consequently, there is a reasoned argument that globally, there should be a collaborative approach to online CSEM offending if governments and criminal justice agencies are to effectively tackle this problem.

#### The Literature Review: Part 2

#### 2.7. Introduction

As a natural progression, part two of the literature review will explore what is currently known about police training and knowledge related to online CSEM offending and cybercrime. In addition, the review will also focus on new technology used in CSEM offending which law enforcement agencies now increasingly investigate. Also, the typologies of online CSEM offenders will be considered along with other online sexual crimes which police routinely investigate. This chapter will begin by exploring the literature surrounding the specific research questions and address the following main headings in order of hierarchy:

- An overview of police cybercrime investigation.
- Police training and knowledge related to online CSEM offending,
- The police E-learning system,
- Police technology adoption'
- Formal accreditation,
- The risk of newer technology related to online CSEM offending,
- The use of social media and the open web in online CSEM offending,
- The typologies of online CSEM offenders,
- Other online cybersex offender typologies.

To begin this part of the literature review, this section explores the literature related to police cybercrime training overall. This inclusion is valid if we are to argue that the literature related to online CSEM investigation per se is limited. In this case, it is prudent to assess the literature to police cybercrime investigation as a whole to provide some context to the overall research question.

#### 2.8. An overview of police cybercrime investigation

Despite online sexual crimes sitting within the family of cybercrime investigation, online CSEM has been neglected (Yar & Steinmetz, 2019). Suppose we look at online CSEM offending through the lens of cybercrime investigation per se. In that case, it could be argued that police officers do not have the experience or the knowledge to deal with cybercrime offences overall (Holt & Bossler, 2016). Owing to this, many police forces feel specialised units are better suited to tackle this problem. Yet, despite this issue, there are significant numbers of police officers and staff involved in the policing of cybercrime who have limited online technical knowledge (Schreuders et al., 2020).

Historically, the lack of cybercrime training for police officers is noted within academic literature. Earlier work by Jewkes & Andrews (2005) argued that despite legislation, the lack of technical expertise and funding within the police service may seriously hamper the efforts to tackle online child sexual abuse and exploitation. In addition, more recent work argues that online training of police officers is crucial as frontline officers are the primary respondents to cybercrime (HMIC, 2017; Holt et al., 2015). In this case, it could be implied that sufficiently trained officers are more able and confident to investigate online child sexual abuse and exploitation.

Despite these earlier claims, it could be argued that the problems related to cybercrime training within the police environment are still evident today. For example, in their needs assessment of a major UK police force, Schreuders et al. (2018) noted that further training was needed around digital technology and the awareness of current apps and technology use. Also, Schreuders et al. (2018) argue that police dealing with child abuse offences should have adequate cybercrime training bespoke to safeguarding. Thus, the evidence suggests that despite the rise in online offending behaviour, some police forces are not keeping pace with training and understanding social media and other online technologies used in CSEM offending.

The evidence thus far may suggest that interactive training methods should be designed to provide officers with a better understanding of cybercrime training and group discussions where ideas can be shared (Hadlington et al., 2018). Notably, one comment regarding Hadlington et al. (2018) relates to the generalisation of their study, which explores cybercrime training overall rather than explicitly concerning online sexual offending. A further limitation of Hadlington et al. (2018) related to this study involved the participants, who did not include detectives from CID departments or similar specialised units.

Although similar, Holt et al. (2019) explored whether there was a significant difference between participants' knowledge of cybercrime training and investigation based on rank, department, whether they were CID or uniform, sex, race, and age. Holt et al. (2019) also noted differences in how detectives and uniform constables perceived online crimes based on their roles. For example, uniform constables attached to CID were more likely than officers in frontline uniform roles to understand the seriousness of some online crimes, including harassment. Similarly, detectives were more likely to understand that CSEM offences occurred more often than 'real word' crimes (Holt et al., 2019). Whilst acknowledging these issues, it is perhaps unfair to suggest that officers in all police forces are disproportionately trained to investigate cybercrime offences.

Referring to this problem, Hinduja (2007) suggests that detectives and police inspectors are effectively better at investigating cybercrime offences due to the technical and complex skills often associated with online crimes. Yet, in contrast, Holt et al. (2019) found that police uniform constables were often the main factor in the initial response to cybercrime investigations. Interestingly, Holt et al. (2019) also noted significant differences among young male officers with a formal education who reported better digital skills than their contemporaries. In addressing these issues, Paoline, Terrill & Rossler (2015) claim that due to the extended role of technology within the police and management expectations, understanding the effects of university graduates has become more relevant.

When focusing on the lens of police cybercrime investigation training, Schreuders et al. (2020) have highlighted several issues, including the need for additional knowledge and training regarding digital technology, the awareness of popular social media apps, and improved learning on social media and online harassment. This evidence suggests that gaps in online technical and social media exist in some front-line police officers. At the same time, it is noted that some uniformed police officers and sergeants who participated in Sheruder et al.'s (2020) study may not have served in frontline investigatory roles, which may have affected their perceptions of reported crimes. Given this argument, further exploration is needed in this area involving officers who are front-line CSEM investigators.

Other issues of note within the literature also included ensuring that officers who dealt with online investigations had the appropriate training and support, explicitly concerning cybercrime and child safeguarding. Evidencing this, Lee et al. (2019) pointed out training concerns relating to senior officers by citing that two-thirds of their sample of 155 police inspectors claimed to have had no training regarding online crimes. Notably, the study participants were police inspectors rather than frontline investigators involved in day-to-day criminal investigations, a factor which may have also influenced the perception of online sex crime offences.

In their scoping review and workshop discussions, Johnson et al. (2020) also investigate these concerns, highlighting management issues regarding technologically driven cybercrime investigation. These views also surfaced in other aspects of their study, suggesting that digital training is aimed at frontline investigators rather than senior leadership.

In support of this claim, Johnson et al. (2020) also noted that in some serious crime cases, the leadership and direction were driven by senior officers with limited knowledge of cybercrime. On these grounds, the literature suggests that there is a compelling case for senior leadership, particularly within online CSEM investigation to understand and promote the fluid nature of online sex crime investigation through training and continual personal development.

After exploring the literature related to police cybercrime investigations, it is prudent to scrutinise the literature regarding how police officers who investigate online CSEM offences are trained. After all, the main focus of this study is to explore the responses to technology-driven changes in online CSEM offending.

## 2.9. Police training and knowledge related to online CSEM investigations

Digital technological advances have created new and sophisticated methods for individuals to expand their online offending behaviour (Fortin, Paquette & Dupont, 2018). Moreover, the internet is now the primary platform for possessing and distributing child abuse images and sexual exploitation (Horsman, 2017). In addition, many online CSEM offences are undertaken via social media apps and the open web (Internet Investigation Report, 2020). In response to how police forces investigate these offences, some authors have expressed marked differences in the online training and knowledge of CSEM offending. Accordingly, referring to Leukfeldt et al. (2013), all police officers are primarily trained to deal with physical offences, while the investigation of online offences is often frustrated by their inability to investigate these crimes effectively.

An issue presented by Leukfeldt et al. (2013) argues that the primary investigation focus for police is fraud and hacking offences instead of online sexual crimes. On the contrary, Leukfeldt et al. (2013) do acknowledge the importance of improving police officers' knowledge of high-impact online offences. Yet, growing evidence suggests that criminal justice agencies and criminologists have neglected to understand police officers' willingness and readiness to investigate cybercrime effectively (Bossler et al., 2019). To that end, a more qualitative investigation is called for to provide valuable insights into how police officers view their ability to respond to online crimes alongside adopting new policies and working practices (Holt et al., 2019).

To understand online crime investigation, one must first analyse what terminology is used by academics, police forces, government, and industry. Over several decades, various scholars have used different terminologies to describe online offending in all its forms (McGuire, 2019). For consistency, this thesis will use the term 'cybercrime' when discussing the literature. First, it is essential to understand the scale of the problem relating to online child sexual exploitation and abuse.

The Independent Inquiry on Child Sexual Abuse (2020) (IICSA) estimates that 14 million children in the UK are under 18. Ergo, many of these children use the internet and are at risk of being exposed to individuals who commit online facilitated sexual offending (IICSA, 2020).

Recent evidence by Brennan, Meridan & Perkins (2017) suggests that the rise in adult-initiated online sexual offending has created significant challenges for law enforcement agencies in tackling this problem. In addition, several studies have also revealed that the internet is now a significant resource for offenders to facilitate the sexual exploitation, grooming, and abuse of children (Beech et al., 2008; Elliot & Beech, 2009; Schell et al., 2007). Moreover, Balfe et al. (2013) draw further attention to this problem by arguing that criminal justice agencies should be aware of the methods offenders use to offend and what technologies are used to exploit or abuse children. On this basis, Schreruders et al. (2018) argue the need for appropriate cybercrime training for staff employed within safeguarding roles, as some possess limited technical knowledge regarding online offences analysis.

Recently, the most common problems facing the police response to cybercrime investigation include knowledge, training, and procedures (Shreuders et al., 2018). Additionally, Yar (2013) points out that internet sex offences are unusual compared to other forms of online offending in that they are investigated much differently from other forms of online crimes. For example, online offences differ from physical crime instigations due to the hierarchies of crime and the perceived differences in seriousness, urgency level of risk, the vulnerability of victims and the level of risk and harm caused. Having said that, to analyse the literature surrounding cybercrime investigations, it is essential to separate online CSEM offending and general cybercrime offences, including fraud and hacking.

To begin, a sizable proportion of literature relating to police cybercrime training does not include online CSEM offences. For instance, in their qualitative exploration into police officers' experience of cybercrime, Haddington et al. (2018) primarily discuss overall cybercrime training such as fraud and hacking. Similarly, Cockcroft et al. (2018), in their work on police cybercrime training, again do not focus on online child sexual exploitation offending but on cybercrime overall. Additionally, Koziarski & Lee (2020) also explore evidence-based policing relating to cybercrime as a whole and not online CSEM and abuse.

However, despite highlighting the discrepancies in police cybercrime training, Burrus et al. (2022) noted that not all police officers are sufficiently prepared to meet the growing response to cybercrime investigation.

When further exploring the literature, the evidence suggests that police officers often lack specialised knowledge and training when investigating cybercrime offences. Simultaneously, it is unfair to suggest that no attention is devoted to cybercrime training related to online CSEM offences. For instance, Schreuders et al. (2018), while focusing on general cybercrime investigation needs, also devote attention to online training related to CSEM and safeguarding. Conversely, despite these inclusions, it is still noted within the literature that online CSEM offences highlight the deficiency within specialised online training for police officers (Senjo 2004; Holt & Bossler 2012; Hinduja 2004).

When exploring the training of police officers, attention should also focus on the primary method in which training is delivered. Accordingly, the next section is devoted to the police online E-learning system.

### 2.10. The police E-Learning training system

Much of the training that police officers receive relies on e-learning platforms (College of Policing, 2021). The Managed Learning Environment (MLE), provided by the National Centre for Applied Learning Technologies (NCALT), now College Learn, is an alternative to classroom-based training. It is widely recognized that police officers and staff must engage in continual professional development to meet the increasing demands of operational policing (Alexandrou and Davies, 2002; College of Policing, 2018; Honess, 2020). Under the circumstances, it could be argued that the online learning platform is flexible in terms of content delivery and does not require face-to-face instruction.

"The online learning platform enables training packages to be easily distributed in a manner in line with changing operational demands" (Honess, 2020, p.3). The College Learn online training system involves interactive online learning sessions where applicants are tested on their knowledge at the end of each session (College of Policing, 2021). Concerning police training overall, Hadlington et al. (2018) highlighted some of the critical issues of police training methods relating to cybercrime, including a lack of specialist resources, knowledge, practical training and the ineffectiveness of online training.

Considering this, Schreuders et al. (2018) acknowledge the need for appropriate online training for staff engaged in child safeguarding and a consistent and effective management approach.

When exploring the police E-Learning system, the majority, if not all, police officers often use this organisational online learning platform, yet despite the need for quick and cost-effective training methods, the online learning forum has come in for some criticism. In their study, Hadlington et al. (2018) claimed that interviewees viewed the NCALT learning platform as "ineffective and outdated". Bearing this in mind, previous research by Boulay et al. (2008) also questioned the effectiveness of e-learning and employment-related training. Consequently, e-learning does not necessarily guarantee practical or cognitive engagement for staff (Garrison & Cleveland-Innes, 2005)

Controversially, participants in Schreuders et al.'s (2020) study described the use of police e-learning training packages as "easy to pass without any evidence or any in-depth understanding of the content". In addition, Hadlington et al. (2018) cite participants describing NCALT as being "rubbish," "ticking a box," and "terrible." Moreover, Honess (2020, p.7) also observed that officers were often unmotivated to complete mandatory e-learning courses, claiming that its content "is neither useful nor interesting" This being so, it could be argued that e-learning packages should have some form of input from the officers and staff who use them to ensure they are current and fit for purpose. Despite this, Hadlington et al. (2018) argue that NCALT training related to cybercrime training fell 'well short' for many officers. So, an argument exists which suggests that online mandatory police training should be valid, relevant, and engaging for officers and staff.

So far, evidence suggests that the NCALT e-learning system is outdated and not engaging enough with officers feeling that it was a mandatory task to be done as quickly as possible (Hadlington et al., 2018). Also, Hadlington et al. (2018) argue that the NCALT online learning system is ineffective in the fluidity of cybercrime training. Having said that, despite the criticisms of the College Learn or NCALT system, it is widely accepted that police officers must engage in continuous professional development (CPD) to address the demands of operational delivery (College of Policing, 2018; Honess, 2020, & Alexandrou & Davis, 2002). Because of this, it could be argued that the cost of online learning sessions far outweighs the resources and time spent in classroom-based learning sessions (Benson & Powell, 2015).

The evidence discussed so far argues that while there is a place for e-learning, these packages must be tailored to meet the officer's needs, ability, and role. Suitable e-learning packages for online sexual crime units could include information on Tor networks and onion routers, peer-to-peer sites (P2P) and the child abuse image database (CAID) system, and signposting to organisations, including the Internet Watch Foundation and National Centre for Missing and Exploited Children (NCMEC). Despite this, as online digital technology is fluid and fast-changing, it would be challenging to create a suitable e-learning package for online sex crime investigations and cybercrime investigations. Resultantly, it could be suggested that police senior leadership must also direct officers to self-learning and continuing personal development (CPD) regarding the changing nature of online digital technology or implement suitable accredited training. This being the case, an argument exists that e-learning packages have a place in learning and development but should also be related to CPD and self-directed learning.

The next sub-section explores the use and adoption of technology within the police. This subject is an important aspect of police training and knowledge as technology adoption related to online CSEM investigation is lacking in academic literature. Despite this, Rossler (2019) claims that police technology is a core principle that shapes the policing role, and the adoption of police technology is connected to successful police reforms.

# 2.11. Technology adoption models and theories related to police training

When exploring the training and knowledge of police officers and civilian investigators, it is essential to explore the phenomenon of police technology adoption. After all, police officers and staff working in CSEM investigations deal with online technology daily. Thereupon, this section briefly explores the various models of technology adoption used by both industry and the police. The literature on technology adoption overall is vast and extensive, dating back many years, (Abbas & Policek, 2021; Escamilla & Reichert, 2019; Teherdoost, 2017; Lindsay, Jackson & Cooke, 2011). Nevertheless, to understand technology adoption, we must first look at the origins of this concept.

Pioneering work by Rogers & Beal (1957) devised the original concept of how personal influences can affect the adoption of technological change and claimed that individuals accepting new change involve complex acts in which the person can understand and distinguish each stage of the process. In addition, Rogers & Beal's (1957) process involved five stages as follows: The awareness stage, where the individual becomes aware of a new idea; the interest stage, where the person seeks out further information on the idea; the evaluation stage; where the individual creates a mental trial of the innovation; the trail stage, which involves small stage experiments of the innovation and the adoption stage which involves large scale and continued use of the innovation.

Later work by Rogers (1995) argued that innovation is an idea or an objective perceived as a new concept by an organisation or a group. Additionally, Rogers (2003) also argued that the diffusion of innovation is not an immediate process but rather a series of actions that occurs over time and can involve a series of proceedings, which may include rejection of the process. Accordingly, organisational resistance or rejection within organisations can include an individual's resistance to change and the age and attitudes of the users (Hircheim & Newman, 1988; Markus, 1983).

When discussing technology adoption, Rogers (1995) defines this as a series of actions in a societal change where innovation is exchanged or shared through a period by various channels amongst members of a social system. Moreover, Rogers (1995) argued that a person's decision to reject or adopt technology is framed by several stages which begin with an awareness of the technology and creates an attitude towards innovation. Because of this, the individual could decide if they will adopt or reject the technology, implement it and finally confirm their decision.

Rogers (2003) described a five-part process of innovation adoption where individuals decided to adopt or reject recent technology. These steps included creating knowledge about how and why the technology works; being persuaded about its value; deciding if to adopt the innovative technology; using it and seeking support to confirm its benefits. Rogers's (1995) theory of technology diffusion adoption has been applied in several other professional practices, including healthcare, where it has been used to implement research-based practice and new standards of care relating to computerised care systems (Landrum, 1998; Lekan-Rutledge, 2000; Lee, 2004).

Due to this action, Rogers' (1995) theory could also be applied within a policing environment when considering technology adoption strategies.

In their study on computerised crime mapping, Weisburd & Lum (2005) claim that the diffusion process can be captured more efficiently by focusing on police units that are more likely to be early adopters of technology and innovation. Also, Bullock et al. (2021) highlight the issues of problem-oriented policing, drawing upon concepts on the diffusion of innovation (Rogers, 2003; Greenhalgh et al., 2004). Yet, as Bullock et al. (2021) point out, although technology adoption theories such as Rogers (2003) have many advantages, there are also some negative aspects which suggest that adopting recent technology and ideas is often difficult, especially in problem-orientated policing.

The College of Policing (2023) defines problem-orientated policing as a specific approach to developing targeted interventions that can be applied to any crime. Furthermore, the model assumes that by identifying a problem and understanding the leading cause, the solution developed to tackle the problem will be effective. Thus, technology adoption can be successfully applied in problem-orientated policing, but only through careful moderation and analysis. Consequently, when exploring other frameworks and models, it is important to note that several frameworks and technology adoption models have been developed to analyse user acceptance of recent technology (Taherdoost, 2018).

Despite some attention being focused on Rogers (2003; 1995), it should be noted that other technology adoption theories exist, and it is worth mentioning some of them in this context. For example, other technology adoption models include the Technology Acceptance Model, Organisational Choice Framework, Coping Theory, and the Coping Model of User Adaptation (Baudry & Pinsonneault, 2005; Abbas & Policek, 2020; Escamilla & Reichert, 2019; Taherdoost, 2018; Lindsay, Jackson & Cooke, 2011). When analysing other technology adoption models, the Technology Acceptance Model (TAM) and other variations, TAM 2, TAM 3, and TAM 4, are the most used models in industry and other organisations for understanding the circumstances that assist in accepting and adopting technology (Lindsay, Jackson & Cooke, 2011).

The original TAM model identifies several concepts that assist in integrating technologies into organisations and identifying why users reject or accept the technology (Davis, 1989). Also, the TAM model suggests that when individuals are provided with new technology, several factors influence their decision-making regarding using it (Lindsay, Jackson & Cooke, 2011). Resultantly, empirical research demonstrates the TAM model's effectiveness in different settings with consistency, reliability, and replication (Money & Turner, 2004; Huang Lin & Chuang, 2007; Liang, Xue & Byrd, 2007; Chau & Hu, 2002).

The TAM 2 model, Venkatesh & Davis (2000), is slightly different in that it incorporates social influences and cognitive developments. Moreover, it considers other factors, including job relevance, quality of output, and results. Similarly, in TAM 3, Venkatesh & Bala (2008) combine TAM2, Venkatesh & Davis (2000) and include "computer self-efficiency", "computer anxiety", "perception of external controls", and "computer playfulness".

Likewise, Lindsay, Jackson & Cooke (2011) provide further definitions of the attributes of TAM3 by describing them as follows: "computer self-efficacy" involves the self-belief of an individual with the ability to perform a task, and "perception of external control" decides if an individual believes that the organisation has the necessary technical support available to them. Also, "computer anxiety" involves the perceived level of fear individuals may face when using a new system, "computer playfulness" explores the motivation of individuals for using new technology, and "perceived enjoyment" is understood as the extent the satisfaction of using new technology has on the user (Lindsay, Jackson & Cooke, 2011).

Nonetheless, several differences are noted when looking at technology adoption through the lens of police and criminal justice agencies. For example, Koper, Lumm & Willis (2014) argue that police organisations often fail to use technology for crime reduction or to achieve other goals like improving community legitimacy. This argument suggests that although police should be encouraged to adopt new technological approaches, they have limited access to research to determine how these approaches work (Engoto et al., 2017). Finally, using new technology is only beneficial if officers are appropriately trained in adopting innovations (Sausdal, 2018).

So far, the literature suggests that the technology adoption process is not a panacea for adopting innovations but a functional theory that can be used by organisational leadership to employ new technology and increase efficiency. Despite this, senior leadership within policing should be mindful of the many technology adoption theories available and, these should be employed by those best suited to their needs. To conclude, the literature suggests that for interventions to be successful, there is an argument for police leadership to embrace academic theories of learning and other concepts related to technology adoption, thus enabling effective service delivery.

The following section examines the concept of formal accredited training for police officers and staff working in online CSEM investigations. Given the serious nature and expertise of their role, there is a valid opportunity for debate around this issue As such, it is important to review the literature in this area to provide further evidence and debate on this matter.

#### 2.12. Formal accreditation for staff working in CSEM investigations

The literature has identified an area of interest within police officers' training related to formal accreditation for those working in CSEM investigations. While conducting the literature review, the researcher noted minimal references regarding the formal accreditation of online sex crime investigators. Pioneering work by Stambaugh et al. (2001) argued for the certification of uniform officers and forensic scientists when dealing with and investigating 'electronic crimes', while Rogers & Seigfried (2004) also agreed with the need for professional accreditation in cybercrime and forensic investigations. Even so, despite this early work concerning cybercrime, there is limited academic evidence relating to accreditation for officers working in online CSEM investigations.

On the other hand, Schredures et al. (2018) argue that official accreditation and qualifications relating to cybercrime investigators might become problematic as less formal training and information sessions may become overshadowed. One challenge to this claim is that Schredures et al. (2018) relate explicitly to cybercrime investigation and not online sex crimes per se. Thereupon, this phenomenon is analysed to understand the benefits of accredited training for online sex crime investigators. So, before this, one must first analyse this concept's history to understand the arguments for and against accredited qualifications for online child abuse investigators.

To begin, earlier work by Button et al. (2007) explored the collaboration between police forces and universities to create training packages for counter-fraud specialists accredited by the university. Moreover, Button et al. (2007) highlight how police were increasingly being left behind in the accreditation of fraud investigators by organisations including the NHS, Department for Work and Pensions (DWP) and HMRC. In this respect, police forces and the UK government allowed officers to attain national accreditation as fraud investigators within the policing service.

As with online sex crime investigators, not all officers are trained to an equal level of specialism. In support, Gilmour (2021) highlights that not all police investigators receive specialist training in fraud and economic crime compared to colleagues in Economic Crime Units (ECU). Similarly, not all police officers are trained to the same level as front-line online sex crime investigators.

Traditionally, police officers usually spend a certain amount of time as a front-line uniform constable before applying to become a detective, yet it is accepted that currently, there are two methods of becoming a police detective: progressing through the uniform ranks and the direct entry detective scheme (The College of Policing, 2023). As such, the direct entry detective scheme differs from the more traditional route as it involves completing the two-year Detective Constable Degree Holder Entry Programme (DHEP) where trainees spend most of their time in front-line policing (Metropolitan Police, 2023).

Before analysing the role of police detectives, it is helpful to understand their roles and responsibilities. Illuminating this, Johnson, Turner & Silverstone (2023) suggest that detectives are expected to use theoretical and analytical skills, knowledge, and experience to adopt professional development concepts and liaise with other staff, including those in the remit of technology, science and law. Also, police detectives are accredited by holding the PIP Level 2 (Programme for Investigatory Skills) investigators course accreditation.

According to the College of Policing, PIP level 1 allows accreditation for priority and volume crime investigations, including low-level theft and fraud cases. In contrast, PIP level 2 relates to more serious and complex crimes and investigations (College of Policing, 2023). As discussed, some detectives are trained at PIP level 2, however, the concept of direct entry detectives and police Inspectors has attracted some criticisms.

For example, Kirby (2018) claimed that the Police Federation, which represents rankand-file officers, argued that the direct entry detective scheme was unnecessary as the current programme was more able to recruit high-quality detectives. Yet, despite initial criticisms, five years after its conception, the direct entry detective programme is now broadly accepted by the police leadership and the rank and file.

When discussing accreditation for officers working in online sex crimes investigation, the Specialist Child Abuse Investigators Development Programme (SCAIDP) should be mentioned. This course is specific to detectives and civilian investigators responsible for investigating and supporting victims of child abuse and associated offences (College of Policing, 2023). Moreover, Freedom of Information Requests from three other major UK police forces, (Appendices, A, B and C) highlight the differences in police training related to online CSEM investigations.

Accordingly, there may be various reasons why some police forces choose not to include SCAIDP training for officers involved in online sex crime investigations, which may include the differences in online sex crime investigation, including the 'cross-national nature' of online child abuse, as the offender and victims of these crimes may reside in different locations and authorities (Broadhurst et al., 2020).

Also, the nature of investigating online CSEM may not involve the witness interview of the children in the images as they are not often 'first-generation images' but have been shared thousands of times over many years (Broadhurst, 2020). Other reasons officers in online sex crime units may fail to undertake SCAIDP training could relate to cost and time factors. In justification, the SCAIDP course lasts five days and costs an average of £750 per candidate (College of Policing, 2023). Inevitably, as policing roles become increasingly fluid, officers may not remain in their current role or position indefinitely due to promotion or upskilling.

Spoher et al. (2010) highlight this problem by arguing that changing job roles is essential for individuals to enhance their quality of life and is now considered the norm in everyday working life. Similarly, earlier work by Pumpian et al. (1997) claims that models for career development assume that changing roles and jobs is an essential part of career development.

In consideration of this, there are numerous reasons why police officers leave their current profession, including retirement, transferring to other roles, and resignation (Cooper & Ingram, 2004).

Given these arguments, one could perhaps understand why leadership within online sex crimes policing may be reluctant to send their staff on courses such as SCAIDP due to cost and time resources. Then again, there is some debate for police officers and staff to hold accreditation suited explicitly to online sex crime investigation. Moreover, it is worth noting that each of the 43 police forces in England and Wales is run as separate entities differing in size and budgets related to funding and training (Home Office 2021). In addition, although each of the 43 police forces in England and Wales now has dedicated cybercrime units dealing with cybercrime, they are not dedicated frontline online sexual crimes units (Public Technology Net, 2019). As such, the evidence from the literature would suggest that accreditation for officers and staff working in online sex crime investigations is beneficial to good working practice on a case-by-case basis based on the size of the unit, the level of CSEM referrals and available finances.

Thus far, the literature review in part two has explored the concept of police training and cybercrime investigation. However, it is also important to understand the types of online sexual and CSEM offences that police officers working in this field investigate in the course of their duties. This inclusion is justified as understanding the types of online offences provides some understanding of policing needs related to their training and knowledge in this area. In a similar vein, exploring the literature related to the typologies of online CSEM offenders is crucial in our understanding of this phenomenon and how police officers are prepared to deal with these offences through their training and knowledge. Subsequently, the next section will explore the literature regarding newer technology used in online CSEM offending, including live-streaming abuse and deep-fake.

## 2.13. The risks of newer technology in online CSEM offending

When investigating live-streaming offences, traditionally, police investigators often relied on money transfers and call logs to gather evidence of live abuse (EPAT, 2018). Even so, the literature will suggest, that with the rise in live time applications, such as Zoom, Messenger and WhatsApp, the evidence chain for live streaming offences lessens dramatically unless the live stream abuse was recorded, saved or shared.

Accordingly, as live-streaming offences occur in real-time, the offender is not required to store the footage, making detection by law enforcement agencies complex (Thorne, 2016).

Additionally, live-stream offenders do not need to risk detection by organising live webcam abuse in countries such as the Philippines, where they can sexually groom children via open social media platforms. Data from the IWF report that it was "uncommon" to encounter child abuse videos captured by live streams featuring Southeast Asian girls, but rather "white girls" from "affluent Western backgrounds" (IWF, 2018). For that reason, there is an argument for exploring the rise in live-stream abuse on open platforms, social media, and live video services.

Virtual Reality (VR) in CSEM exploitation is another concern that has received minimal attention. Moreover, VR has become more affordable and was previously used by individuals for 'traditional pornography' (Takahashi, 2016). Furthermore, according to Takahashi (2016), VR pornography can also deliver an intimate viewing experience for users rather than a traditional third-person voyeuristic standpoint. Yet, despite the legalities of VR in legal pornography use, some offenders may use VR for child sexual offending purposes. Moreover, Rutkin (2016) and Maras & Shapiro (2017) claim that when used with child sex abuse material, VR may cause online-only offenders to transition to contact child sex offending behaviour. Accordingly, there is an argument for further academic scrutiny related to VR CSEM offending.

In contrast, there is a contentious school of thought amongst some practitioners that VR can be used to assess risk in sex offenders. Illustrating this, Fromberger, Jordan & Muller, 2018) and Kip et al. (2019) suggest that VR can expose offenders to virtual situations to observe their behaviour without endangering others while assessing their decision-making processes. In addition, offenders can be monitored when using VR in child interaction scenarios without posing a risk to children (Nee et al., 2019). All the same, despite the usefulness of VR in offender risk management, caution is noted as decisions are extremely difficult for practitioners, given the severe consequences of any wrong decisions (Fromberg et al., 2018).

Finally, in this overview of newer technology used in CSEM offending, there should also be mention of pseudo-imagery and deep-fake pornography. Traditionally, pseudo-imagery in CSEM offending involves a child's face being digitally manipulated onto an adult body to produce a sexualised image (Yar & Steinmetz, 2019). A definition provided by Meskyes et al. (2020) suggests that deep-fake technology involves face swapping, which enables the creation of fake images or videos that appear very realistic. Deep fake images can be created using open-source software libraries and social media platforms, including Facebook, YouTube, and Instagram (Ratner, 2021). In short, this makes it easier for deep-fake technology to be used by specific individuals for illegal purposes.

Despite the concerns regarding deep fake technology, there is an argument for the positive aspects of this phenomenon. Westurlund (2019) contends that deep-fake technology can be used positively in many industries, including education, digital communication, health care, business and fashion. Nevertheless, despite the usefulness of deep-fake technology, there is still a concern regarding its use in CSEM offending. For example, although most deep-fake posts are pornographic, most societal attention to deep-fake technology is currently devoted to political issues, revenge porn against women, blackmail and harassment involving celebrities. (Geiseke, 2020; Karasavva & Noorbhai, 2021; Maddocks, 2020; Mahmud & Sarmin, 2021; Westerlund, 2019). Thereby, the literature suggests that the academic contribution of CSEM offending and deep fake technology is minimal and requires further investigation.

While discussing the literature surrounding newer technology in online CSEM offending, it is also important to address the issues regarding how most online CSEM offending is carried out by the offenders. On this account, the next sub-section will look at the use of social media and the open web in online CSEM offending.

## 2.14. The use of social media and the open web in online offending behaviour

Contrary to public perception, a lack of technical knowledge is not a barrier to accessing the 'dark web' as users do not usually require real expertise to hide their identity on the internet (Davis, 2020). In addition, most CSEM offenders do not employ sophisticated technological countermeasures to hide their online activity (Balfe et al., 2015).

Interestingly, as Steel et al. (2022) argue, individuals previously convicted of CSEM offences were likelier to use technological countermeasures to hide their online activity, yet the countermeasures used were less sophisticated, with encryption usage higher.

Today, almost all reported crimes involve using the internet, including social media and other digital platforms. (Seigfried-Spellar & Leshney, 2016). Furthermore, individuals using the open web to access abusive images of children to facilitate online sexual crimes suggests that policing this environment is often difficult due to continually changing technical developments (Johnson et al., 2020). In light of this, it could be suggested that police and criminal justice agencies may have some difficulties monitoring all the platforms used to engage in offending behaviour.

In quantifying this problem, British Telecom (BT) research reported that in 2015, there were 36,738 attempts to access child sexual abuse images every 24 hours in the UK (IICSA Investigation Report, 2020). Furthermore, in 2018, several police forces recorded more than ten grooming offences per day on social media sites, with Facebook, Snapchat, and Instagram being the most used. Moreover, recent evidence by Kent and West Midlands Police also reported that offenders' three most common digital platforms in child abuse cases were Facebook, Snapchat, and Instagram (IICSA, 2020). Similarly, participants in the Independent Inquiry into Child Sexual Abuse, Learning about Online Sexual Harm (2019) repeatedly cited Snapchat, Facebook, and Instagram as the leading platforms where online sexual harm and harassment occurred.

In exploring previous work related to this problem, Ashurst & McAlinden (2015) suggest that social media apps are the primary method for online grooming and sexual exploitation with most of the access to these social media platforms being used by smartphones or tablets. Additionally, the Organisation for Economic Co-operation and Development reported in 2015 that 94.8% of 15-year-olds living in the UK use social media apps before and after school (House of Commons Science and Technology Committee, 2019). To this end, children aged 8 to 11 now typically spend up to 13 hours per week online, and 70% of 12 to 15-year-olds have a social media account profile (Ofcom, 2018).

The evidence thus far outlines that, contrary to the populist view, children are more at risk of online sexual harm through social media sites than on other digital platforms (NSPCC, 2019). Despite the evidence regarding the open web and social media platforms used in CSEM offending, there should also be a mention of hidden Tor network platforms or the so-called 'dark web.' The 'dark web' is a network of devices that uses cryptographic protocols to communicate anonymously with others without revealing the user's location (Biddle et al., 2002). Even so, one argument would suggest that hiding one's identity online can be a positive aspect in some cases, such as viewing pro-democracy literature in totalitarian regimes (Cole & Chowdry, 2021). In that event, society should not automatically assume that the 'dark web' is used for nefarious purposes.

Despite some positive ways in which hidden networks can be used, previous research by Owen & Savage (2015) found that the most frequent content on the dark web was indecent images of children. Moreover, to access illegal content on the 'dark web,' offenders use 'Tor' networks or 'onion routers', creating new chains of servers with added encryption keys (Cohen-Almagore, 2013). Also, despite the complex idea of hidden services, downloading the software is quite straightforward and in some cases, using free browsers (Becker & Fitzpatrick, 2018). Because of this, the covert internet method employs a global network of devices that use a cryptographic protocol to enable users to communicate anonymously without revealing their location (Davis, 2020).

In essence, Tor browsers allow users to connect to web pages anonymously by deflecting connections at random intervals, allowing the Tor nodes to confuse the user's IP address, making detection difficult (Davis, 2020). Moreover, online sex offenders can avoid leaving a traceable digital footprint by employing other methods, such as virtual private networks (VPN) and Dynamic Domain Systems (DDNS). Additionally, this technology keeps offenders hidden from law enforcement agencies and Internet service providers (Alazab & Broadhurst, 2016). Thus, internet service providers and criminal justice agencies face increasing difficulties and barriers in identifying offenders and their locations using hidden services (Davis, 2020).

Finally, as far as Cohen-Almagore (2013) is concerned, criminal justice agencies should better understand the technology and techniques of online child sex offenders to tackle this critical societal problem. So, as online technology develops and improves, there is a convincing argument for better training and knowledge for officers and staff investigating online CSEM offending. Further reading on the digital pathways used to commit online offences is discussed by Beech et al. (2008; Gallagher, 2007; Kierkegaard, 2011; & Mitchell et al., 2011).

Online safeguarding organisations and law enforcement agencies must target specific individuals to understand their offender traits and behaviours to reduce offending in this area (Napier, Smith & Brown, 2020). Therefore, the next main section of this chapter explores the literature surrounding the typologies of online CSEM offenders and how their behaviours and use of digital platforms have been shaped by the developments in online technology. This topic is valid if we are to understand the behaviour of the individuals who engage in CSEM offending and how police training and knowledge can effectively respond to this.

#### 2.15. The typologies of online CSEM offenders

When exploring the origins of online criminality, Ogburn (1964) predicted that emerging technology has a powerful influence on human behaviour. Understanding child sexual exploitation offending behaviour is vital in identifying the inconsistencies within criminal justice training, guidance and responses. For instance, online sex offenders are much different from contact sex offenders as they exclusively use the internet and other related technology to commit their offences (Seto, Hanson & Babchishin, 2011). That being so, when discussing using the internet to sexually offend, it could be suggested that the internet has helped to create specific deviant groups, which would be restricted in their behaviours in the real world (Quinn & Forsyth, 2005).

As the literature on the typology and characteristics of adult-initiated child sex offending is vast and dates back many years, this thesis has summarised the current literature to reflect the most common types of CSEM online offenders. Previous studies have reported that online CSEM offenders are almost entirely male, aged in their late thirties to midforties, employed, and educated (Bourke & Hernandez, 2009).

Also, offenders are likelier to be white and never married (Siegfried et al., 2008; Babchishin et al., 2011). Similar findings related to ethnicity and relationship status of CSEM offenders are also discussed by Meridan, Wilson & Boer (2009; Seto et al., 2010; O'Brien & Webster, 2007). But, as Kirwin & Power (2013) point out, offender profiling is problematic as it may describe individuals who are not CSEM offenders. This being so, it is prudent for practitioners and criminal justice professionals to consider this when investigating related criminal activity (Kirwin & Power, 2013).

It is also vital to mention other CSEM offenders, including 'chat room offenders' or adults who engage in sexualised chat with children and grooming via an online setting such as chat rooms and peer-to-peer sites. Krone (2004), Table 2.5. outlines the various typologies of online CSEM offenders, yet since 2004, technological improvements have created new methods of online offending and changed offending behaviour. This issue will be discussed in more detail in Chapter 6.

Table 2.5. Krone's (2004) Typology of Internet Child Abuse Offenders.

Type of offending	Methods used

**Browsers**- Saves indecent images that they happen across but do not interact with other offenders.

**Trawlers**- Actively seek out images and may network with others.

**Secure collectors**- Engages in high-level online security and may belong to secure child abuse rings.

**Non-secure collectors**- Uses non-secure sources and open content to engage in abusive images.

**Physical abusers**- Sexually abuse children and may record the abuse for personal use but also seek out online child abuse.

By exploring the literature, the emergence of other online offenders is noted such as illegal anime content and individuals who use software to create sexualised images of children. For example, over recent years, the sexual depiction of some characters in Japanese anime who appear to be minors has caused much concern in numerous countries across the globe. In addition, the UK, Canada, New Zealand, and Australia have outlawed fictional depictions of characters under 18 under the definition of child abuse material (McLelland, 2017; McLelland, 2012; Johnson, 2010). Accordingly, the literature suggests that more individuals now use live streaming and VR to offend, which should be considered by scholars when discussing the typologies of online offending behaviour (Renaud et al., 2014; Trottier et al., 2019; Napier, Smith & Brown, 2020; Napier, Teunissen & Boxhall, 2021).

Finishing this section, it is important to note that by identifying online offenders' typology and their use of technology, we can further explore the digital platforms used to carry out their offending behaviour. In support of this argument, Winters, Kaylor & Jeglic (2017) suggest that offenders' use of other communication methods to commit sexual offences has been overlooked in past literature. To this end, the literature suggests that there is a need for further exploration related to online CSEM offenders, their use of technology and how their offending behaviours may have changed. Further discussion on the types of CSEM offending behaviours is explored by Alexy, Burgess & Barker (2005; Walsh & Wolak, 2005; Howitt & Sheldon, 2007; Wolak et al., 2004; Malesky, 2007).

The following section draws attention to other online offenders or those individuals who use technology to carry out their offending behaviours which are not specifically CSEM offences. This inclusion is an important facet of this work as exploring the behaviours of other online offenders allows researchers and policing organisations to understand the differences in online offending behaviours.

## 2.16. Other online cybersex crimes and offending typologies

Like other offending behaviours, cybercriminals may fit into specific typologies. For example, Holt & Bossler (2016) discuss the wide range of cybercrime typologies, including 'cyber-deviancy'. Moreover, Quinn & Forsyth (2013) claim that 'cyber-deviance' encircles online sexual activities, including accessing pornography and engaging in sexualised chat with strangers.

In addition, Wall (2001) provided one of the first online offender-based typologies involving four categories: cyber-trespass, cyber deception and theft, cyber-porn and obscenity, and cyber-violence. Ergo, cybercrime covers the whole spectrum of 'real-world' offending but in the online environment.

When exploring cybercrime offences further, Furnell (2002) describes cyber-trespass as an attempt to use wireless networks and secure devices without permission, either by compromising passwords or other technological means. Cyber-deception or fraud occurs when an individual acquires information or goods online. Cyber-deception can include attempts to gain financial data, which can be used for nefarious reasons (Franklin et al., 2007; Holt & Lampke, 2010). On the other hand, cyber-pornography involves a wide array of offences, including online child sexual exploitation (Holt et al., 2022).

As Gillespie (2019) points out, the internet is now the most significant source of pornography. Furthermore, the internet has enabled content that appeals to any interests, including sexual fetishes and extreme acts such as bestiality, necrophilia, and other paraphilia (Quinn & Forsyth, 2013; Holt et al., 2022). Yet, it is also argued that the internet is now the primary source of accessible legal pornography, with billions of users globally each year (Kuilbert et al., 2021). Suffice it to say that whilst many of these users will access legal pornography, there is an element who will seek out illegal CSEM.

Describing online pornography, Brenner (2011) describes this as including erotic writing, drawings, photos, video, and audio content, however, it is also accepted that in most Western nations, online pornographic content is legal so long as the consumer and those taking part are over 18 and consenting (Holt et al., 2022). Although Brenner's (2011) descriptions of cyber-pornography are still relevant today, technological changes call for amendments in the responses to online sexual offending, including the live streaming of child sexual abuse and the emerging trend in virtual reality.

It is worth mentioning other new and emerging cybersex trends, which include so-called 'revenge porn.' until recent years, most countries, including the UK, had no specific laws to tackle the problem of revenge porn (Fanghanel et al., 2021). Despite this, in 2015, Section 33 of the Criminal Justice and Courts Act (2015) created an offence of sharing and disclosing private sexual images or videos without the owner's consent (CPS, 2017).

However, despite the legislation clearly stating the components of the offence of sharing private sexual images without consent, there is, in some corners, a consensus that this offence should be termed as 'image-based sexual violence' (Fanghanel et al., 2021).

It could be argued that unless any act of violence is used within the images or videos, then image-based sexual violence would not fit into this category. For example, cyber-violence should be mentioned when discussing the phenomenon of cyber-related offences. Cyber-violence can involve any online hurtful or dangerous content that may result in physical and emotional harm (Holt & Bossler, 2016). Accordingly, cyber-violence often involves online content that promotes dangerous and unhealthy behaviours, including self-harm, alcohol or drug misuse, binge eating and pro-suicide websites (Burgess-Proctor, Hinduja & Patchin, 2009; Gillespie, 2019). Additionally, falling into the bracket of online harms are cyberbullying, online harassment, and stalking (Burgess-Proctor, Hinduja & Patchin, 2009; Nobles et al., 2014; Reyns, Henson & Fisher, 2012). Necessarily, as the literature is so vast regarding these subjects, only a cursory overview is provided in this review.

To finish, the radicalisation by extremist groups on the Internet should not go unnoticed in any review of cybercrime offending. Again, there will be a cursory mention as the literature is vast in this area. Online extremism now receives more academic attention than ever (Winter et al., 2020). In addition, research shows that extremist groups are using the internet to spread their ideology online to connect with like-minded individuals with the specific aim of recruitment (Odag, Leiser & Boehnke, 2019). Thereafter, evidence from the Ministry of Justice revealed that most convicted terrorists in UK prisons since 2010 were radicalised online (The Guardian, 2022).

Notably, the extent of online radicalisation is a primary concern for the global community and law enforcement agencies alike. Consequently, constructing a culture of responsibility to tackle online harm should be a collective responsibility of governments, criminal justice agencies, industry, and partners (Morris, 2016). Finally, as Zeiger & Gyte (2020) point out, government and internet providers must be forward-thinking in assessing how digital platforms are compromised and identify future threats to employ proactive countermeasures. Further reading on online radicalisation can be found in (Scrivens, Windisch & Simi, 2020; Khader, 2016; Zeiger & Gyte, 2010; Holt et al., 2015).

#### 2.17. Conclusion

Several key areas related to the initial research question have been explored within this review, however, the most significant aspect arising from the literature review highlights the importance of the technology companies and their contributions to developing online CSEM prevention and detection countermeasures. Secondly, it is noted that the vast amount of academic literature on police training related to cybercrime or cybercrime offences relates to non-sexual offences, such as fraud and hacking, rather than online CSEM offending overall.

It is noted that many scholars within the literature have contributed a wealth of knowledge regarding police cybercrime training overall; however, there are minimal contributions related to police training in online CSEM per se. Thereupon, this is an important area for academics who wish to gain additional knowledge on this subject by way of further studies in this field as arguably, adequate online CSEM training enables police organisations to be better prepared to investigate these offences. Due to this concern, adequate and appropriate training for staff provides them with confidence and a better understanding of online CSEM investigations.

Finally, the literature suggests that traditional online E-training for police staff is not engaging and sufficient to meet the training needs of officers and staff. In addition, formal accreditation for officers working in online CSEM investigations is noted. Given the serious nature of their role should officers who work within online CSEM investigation be afforded accreditation like financial investigators? Despite the literature identifying this area, there are minimal academic contributions related to the issues of formal accreditation for officers and staff working in online CSEM investigations. Suffice it to say that the literature finding, overall, indicates that police officers' training related to online CSEM investigation is inconsistent, given the serious nature of their role.

'Police practices should be based on scientific evidence about what works best'.

(Sherman, 1982, p.2)

## Chapter 3. Methods and Methodology

#### 3.1. Introduction

This chapter explores the study's methods design, which involved the use of semi-structured interviews with participants working front-line in online CSEM investigations and secondary data analysis from the Internet Watch Foundation from 2009-2022. An overview of the research process is duly provided as follows: A review and narrative overview of relevant literature was used related to police knowledge and training in online sexual crime investigation, police technology adoption, typologies of offenders, technology countermeasures used in online sexual offending, police cybercrime training and the history of the internet and online sexual crimes. Semi-structured interviews were conducted with nine police officers and two civilian investigators who worked in online sexual crimes Investigations within a large UK police force.

The data were coded, a thematic analysis was conducted, and descriptive findings were discussed. Then, quantitative data from the Internet Watch Foundation were analysed and coded using a thematic analysis of relevant themes. The phases of the research in this thesis included: Organising and carrying out face-to-face interviews, transcribing the interviews, coding the transcripts; data analysis; sourcing and analysing the secondary data; coding the data; reaching a set of findings and drawing conclusions.

### 3.2. The overarching study question

The overarching research question asks, are police officers keeping pace with technology-driven changes in online child sexual exploitation offending? In addition, there are several underlying sub-questions which support the primary research question as follows: How can police officers be better trained to investigate online child sexual exploitation material crime offences against children; has the evolving nature of online digital technology changed offending behaviour and the policing response to online child sexual exploitation material crimes; are the advances in online technology and social media placing much younger children at online risk through self-generated images and are the technology industries now the primary responders to online sexual crime detection and countermeasures? To this end, this chapter aims to address the methods and methodology used in this work to answer these questions.

#### 3.3. An overview of the study methodology

As with the methods section of a typical social science study, the methods and methodology are crucial aspects of the research process. However, it is also important to discuss earlier in this section the suitability of different methodologies within the research process. For example, this study uses two methods for gathering the data, face-to-face participant interviews and analysis of secondary quantitative data from the Internet Watch Foundation. Other methods of gathering data such as observations, focus groups, surveys and questionnaires were excluded due to the suitability of the chosen methods. Resultantly, secondary data analysis and one-to-one interviews were chosen as the primary tool for the data collection.

Evidencing the reason why this thesis has chosen face-to-face interviews, Ennis & Chen (2012) posit that the function of a one-to-one interview is to gather in-depth knowledge regarding a participant's view of the world, their key information and beliefs about the research subject. This being so, as the researcher was a former police officer it was crucial to obtain a candid account of the participant's perspectives and experiences of working in online sexual crimes investigation which could not be fully achieved using questionnaires and focus groups.

Focus groups and questionnaires were discounted in this study for several reasons. Illuminating this, Smithson (2000) highlights the problems of using focus groups in social enquiry such as dominant group individuals allowing one opinion, and group dynamics creating barriers to controversial perspectives allowing for normative discourse. As the subject of this study relates to the knowledge and training of police officers regarding online digital platforms and social media, it is vital to gain an honest account from the participants. This concept becomes more apparent in Chapter 4, the interviews where participants can provide an open narrative regarding the level of their co-workers' online knowledge and ability.

Similarly, questionnaires have been discounted within this study as they are primarily used in larger and wider populations rather than a smaller specific group (Rowley, 2014). In addition, the use of questionnaires was deemed unsuitable by the researcher in this study, as to gather appropriate data regarding the 'lived experience' of participants other methods are more suitable such as face-to-face structured interviews. To support this argument, although surveys or questionnaires can indicate how people behave in a certain way, they are limited in how or why people act or think as they do (Mathers et al., 1998). Moreover, as Kuter & Yilmaz (2001) suggest, questionnaires usually involve quantitative data and a much more useful for providing statistical analysis while semi-structured interviews create a better atmosphere for participants to become more enthusiastic about the subject matter. Due to these reasons, face-to-face or semi-structured participant interviews were used within this study as they provide rich and in-depth data which cannot be gained by questionnaires alone (Bearman, 2019).

During the analysis of the secondary data, the IWF annual reports from 2009 to 2022 were analysed and involved thematic analysis of quantitative data relating to several themes, which included the rise in self-generated images of children, the changes to the ages and genders of children sharing self-generated images and the changes in online technology and the risk to children. Permission was granted from the IWF to use their data in this thesis (Appendix D). The fieldwork relating to the face-to-face participant interviews of the study took place in police stations in a large police force in England. Semi-structured interviews were conducted with police officers and civilian staff who worked in an online CSEM investigation role.

The interview design of this study involved a series of separate questionnaire forms for use in interviews with online sexual crimes unit personnel and CID officers. In addition, Freedom of Information Requests (Appendices, A, B and C) were obtained from other large police forces in England and Wales regarding the levels of training each police force required for their staff to work in online sexual crimes investigation. This area is discussed in greater detail in Chapter 4, the participant interviews.

As previously noted, this thesis employs a convergent mixed-method process as other means of obtaining data were ruled out due to difficulties in the recruitment of participants due to some issues related to the COVID-19 pandemic. Still, as Gailloux et al. (2022) point out, concerns and fears related to the COVID-19 pandemic can affect participants' willingness to engage in research projects, as such researchers must become more resourceful and imaginative to seek other ways of obtaining relevant data that supports the research question. For this reason, other methods for obtaining data were used, namely utilising both quantitative and qualitative approaches.

When exploring mixed-methods research, Watkins (2023, p.5) defines mixed-methods research as 'the rigorous and epistemological application and the interrogation of qualitative and quantitative research approaches to draw interpretation based on the combined strengths of both approaches to influence research, practice, and policy. Moreover, Table 3.1. Watkins (2023) provides several examples of core mixed methods designs and definitions including convergent mixed methods designs as used in this study. To this end, the researcher has employed a mixed-methods approach to facilitate answering the research question.

Table 3.1. (Watkins, 2023). Core Mixed-Methods Designs and Definitions

Design	Definition
Convergent-	A core mixed-method design where quantitative and qualitative data are collected and analysed concurrently with the findings interpreted collectively.
Exploratory -	A core mixed-method design where qualitative data are collected.
Sequential -	This is followed by collecting and analysing quantitative data.
Analysis	Usually, the findings from the qualitative data are used to make decisions about the collection, analysis, and interpretation of the qualitative data.
Explanatory -	A core mixed-methods design where quantitative data are collected
Sequential	and analysed first, followed by collecting and analysing qualitative data Usually, the findings are used to make decisions about the collection, analysis, and interpretation of the qualitative data.

## 3.4. Ontology

As previously mentioned, this thesis uses a constructionist ontological position. Clark et al. (2021, p.27) describe ontology as the 'study of being' and social ontology concerning the nature of 'social entities'. In addition, Crotty (1998) defines ontology by suggesting that it is concerned with the nature of existence and the structure of reality. Yet, despite these claims, some arguments suggest that ontological and epistemological issues merge. As a result, Crotty (1998) argues that ontological and epistemological issues blend; however, because of this cohesion, there are sometimes difficulties in researchers conceptually keeping ontology and epistemology apart.

There is a consensus amongst some scholars which accept that within ontology, two positions exist, 'objectivism' and 'constructivism', which are used as a lens to consider organisation and culture (Clark et al., 2022). According to Bryman (2004), objectivism causes the social entity to follow an external objective reality independent of the researcher's awareness. When discussing objectivism, Crotty (1989) claims that meaningful entities exist independent of experience and consciousness, with truth and meaning as objects; ergo, careful scientific investigation can attain objective truth and meaning. Given this stance, objectivism argues that individuals may learn the truth about reality through repeated observations and controlled situations (Dieronitou, 2014). Appropriately, this thesis seeks the truth of reality through the narrative of those who work front line in online CSEM investigations by hearing their lived experiences and knowledge.

Given the foundations of objectivism from an ontological perspective, this thesis has adopted a constructionist ontological position. It should be noted that constructionism in this context is far removed from the objectivism approach found in the positive stance (Crotty, 1998). For example, constructionism is usually associated with an ontological position in social objects and categories; it is appropriate for qualitative inquiry. As a matter of course, the concept of the constructionist ontological stance is compatible with the foundations of the thesis, fieldwork, and findings.

Suppose we explore the concept of constructionism within this study. In that case, the constructionist position challenges the perception that organisations and cultures have pre-external realities and that social actors have no method of influencing (Clark et al., 2021). Thereupon, the interpretivism and constructivist perspective views the world as a constructed reality experienced by individuals in their interactions within more comprehensive social systems (Guba & Lincoln, 1985). For that reason, this thesis adopts this stance as the most appropriate ontological position.

## 3.5. Epistemology

According to Clark et al. (2022), several epistemological concepts exist, including positivism, realism, critical realism and interpretivism. It is noted that this study uses an interpretive epistemological approach. Epistemology associated with social research asks the question, what is or should be? In addition, Hamlyn (1995, p.242) argues that epistemology explores "the nature of knowledge, its possibility, scope and general basis." A more direct perspective related to epistemology claims that it is a way of viewing and making sense of the world (Crotty, 1998). Moreover, epistemology reflects our position on what forms valuable and meaningful knowledge. Consequently, epistemology in this study provides the philosophical grounding to decide which type of knowledge is suitable and legitimate.

Although several epistemological concepts exist, interpretivism has been chosen for the current qualitative aspect of the study as individuals and social situations are much different from studies in the natural sciences. Consequently, a different approach is needed, which understands the qualities of people in their social institutions (Clark et al., 2021). To support this claim, Ryan (2018) argues that truth and knowledge are subjective and are culturally and historically based on people's experiences and their understanding of them. Proportionately, it is appropriate that the qualitative aspect of this study adopts an interpretivist approach.

It is prudent to acknowledge that this thesis involves qualitative and quantitative approaches. As Bryman (2010) indicates, the differences between qualitative and quantitative approaches to study by arguing that although qualitative research traditionally adopts a constructionist and interpretive approach, this is not always the case. Also, as Bryman (2010) points out, this theory suggests that the connections between epistemology, ontology, and research methods are tendencies rather than seen as defining connections. For example, Platt (1981) claims that as some social inquiries and studies are based on interviews and questionnaires, it could be suggested that quantitative researchers address meanings. Accordingly, while acknowledging that qualitative research primarily adopts an interpretive approach, researchers must also keep an open mind concerning mixed methods of inquiry.

This thesis adopts interpretivism whilst acknowledging the quantitative aspects of the research. In addition, this study adopts an inductive approach to datum theory and an abductive reasoning approach to the quantitative data. As discussed, a constructionist ontological position and an interpretivist epistemological orientation have been employed within this thesis. Hence, it is prudent to discuss the relationship between constructivism and symbolic interaction within context. Blumer (1962) introduced symbolic interactionism and built upon earlier work by Mead (1934). Language and interaction were critical aspects for Mead (1934) to develop the mind, the self and consciousness. Also fundamental to the principles of symbolic interaction is the view that individuals construct their own and each other's identities through everyday interactions (Burr, 2003). That being so, this thesis accepts that symbolic interaction affects how society and individuals interact through consciousness and the ability to focus on the experiences that emerge from these interactions.

As previously discussed, a constructivist approach is usually found in most research perspectives other than positivist or post-positivist paradigms (Crotty, 1998). Yet despite this stance, symbolic interactionism is not the sole entity of qualitative research per se. For example, Crotty (1998) points out that ethnography, which has its foundations in anthropological theory, has been adopted by symbolic interactionism. As Crotty (1998) demonstrates, symbolic interactionism is just one of several theoretical perspectives arising from an epistemological stance.

### 3.6. Symbolic interactionism related to constructivism

According to Bryman (2004), constructivism states that social actors complete social occurrences and their meanings, implying that social categories are not only produced through social interaction but are always in a constant state of revision. Nonetheless, as seen in Fig 3.1. (Bryman, 2004), how does constructivism relate to symbolic interaction as an interpretivist theory? Blumer (1962) introduced Symbolic interactionism, built on Mead's (1934), earlier work which suggested that mind and consciousness and the relationship between society were based upon the dependency on oneself and others. Subsequently, it is essential to note that Mead (1934) argues that language allows individuals to internalise social interactions to represent it to themselves, thus thinking and reflecting upon it.

Upon further exploration of this theory, Crotty (1998) argues that symbolic interaction between individuals and society arises from the communication and interactions between individuals. Furthermore, Crotty (1998) claims that our ability to reflect on our experiences and self is observed as emerging from these interactions through symbolic interactionism. Keeping that in mind, this thesis involves participant interviews where the voice of social actors in this process is vital. This being so, social interactions and dialogue are essential processes that emphasise social relationships and interactions (Crotty, 1998).

To further explain the concept of symbolic interaction, Bryman (2004) argues that the process occurs in such a manner that the individual continually interprets the symbolic meaning of their environment, which includes the actions of others. Moreover, Blumer (1962) claims that the position of symbolic interaction requires the researcher to capture the process of interpretation through which the actors construct their actions. With that, symbolic interactionism within qualitative studies argues that the central doctrine of theoretical positions, such as symbolic interactionism, is understanding that individuals do not conduct social phenomena alone but learn from each other (Bryman, 2004).

In the context of qualitative enquiry, Blumer (1962) claims that 'symbolic interactionism is distinct to us as individuals because it is in some part what makes us human. As a result, rather than reacting to human action, we as individuals interpret or define it. Mead (1962, p.180) captures the essence of recognising this theory by claiming that "Anything of which a human being is conscious he is indicating to himself the continuous life of the human being; it is a continual flow of self-indications". Yet, despite the philosophical considerations of symbolic interactionism within the constructionist paradigm, it would be naive to suggest constructivism does not have some criticisms.

As Howell (2013) points out, the main criticisms of constructivism involve relativist reduction and self-confutation, where reality is constructed. Thereupon, all constructions are an actual reality. Moreover, constructionist propositions involve multiple interconnected realities, which raise more questions than answers. As a result, the prediction and outcome, cause, and effect, are unlikely outcomes of constructivist research, although the stages of knowledge and understanding can be achieved (Guba & Lincoln, 1985). Based on this, in the constructivist paradigm, the researcher and those being studied continually influence and interact; consequently, the research project has limited possibilities related to generalisation (Howell, 2013).

Turning to the constructionist approach to how levels of understanding are achieved, we must look at the conflict between positivism and hermeneutics, which concerns itself with the theory and method of interpreting human action (Bryman, 2004). As Bryman (2004) points out, the clash between positivism and hermeneutics mirrors the differences between prioritising the explanation of human behaviour, which is the main ingredient of the positive approach to understanding human behaviour and the social sciences. Accordingly, as Bryman(2004) further argues, the contrast in both approaches reflects long-standing arguments that precede modern social sciences' emergence.

Weber (1864-1920) created an approach known as Verstehen, which in his native German means 'understanding'. Posthumous work by Weber (1947) describes sociology as a 'science which attempts the interpretive understanding of social action to arrive at a causal explanation of its course and effects. As Bryman (2004) points out, Weber's (1947) definition is not without criticism.

As such, Bryman (2004) argues that although Weber embraces explanation and understanding, the critical point of 'causal explanation is carried out regarding the interpretive knowledge and understanding of social action as opposed to external forces, which have no meaning for those involved in the social action.

Bryman (2004) posits that Verstehen and the hermeneutic-phenomenological customs do not deplete the intellectual influences on interpretivism. Phenomenology as an intellectual tradition has been primarily responsible for the anti-positivist interpretivist position, and phenomenology, as a philosophical approach, is centred on how individuals make sense of the world, particularly by the person, and can overcome preconceptions to understand the circumstances linked to human consciousness. Regardless, it is accepted that Shutz (1889-1959) first applied phenomenology to the social sciences, where Weber's (1947) concept of Verstehen heavily influenced his work.

Shutz (1962:59) claims that 'by a series of common-sense constructs, they have pre-selected and pre-interpreted this world which they experience as the reality of their daily lives. It is these thoughts and objects that determine their behaviour by motivating it. (Shutz, 1962:59). Here, Schutz states that there is a fundamental difference between the subject of natural science and social sciences. So, as Bryman (2004) argues, an epistemological approach is needed to capitalise upon the differences. In addition, these principles are also noted by Wilhelm Dithy (1833-1911), whose work was concerned with making distinctions between the natural and social sciences by using methods that could be analysed and studied (Howell, 2013). In addition, Dithy created the term' hermeneutic circle' which uses continual interaction between the implicit and explicit. Finally, Dithy (1833-1911) argues that hermeneutics used as a methodology for the social sciences contrasts with the empirical approaches utilised in the social sciences.

It should be noted that Weber's (1864-1920) methodological position emphasised that subjectivity was an essential aspect of research, arguing that human culture and behaviour should become a part of the research process and findings. Despite this, Weber's arguments are not without criticism. An interpretive position adopted by Prus (1996) argues that Weber's orientations are imbedded by much ambiguity, confusion, and contradiction.

Moreover, Prus (1996) also claims that the criticisms of Weber and Verstehen do not apply to the viewpoints and opinions of certain people and how they accomplish their daily activities on a here-and-now basis (Serge, 2014). Consequently, Weber's (1947) concept of verstehen is not wholly adopted within this thesis per se but instead used as a foundation for social inquiry.

To support this stance, Prus (1996) claims that Weber does not consider the significance of symbolic communication and meaningful social interaction at length. Also, as Ekström (1992) argues, the interpretation of Weber's methodology has been isolated in the discussion concerning methodologies in the social sciences, which has opened a debate in the controversy and understanding of causal explanation between qualitative and quantitative methods. Subsequently, some scholars ignore or overlook Weber's theory of verstehen sociology as a concept of causality (Herva, 1988).

One explanation for scholars in the social sciences overlooking Weber's (1947) theory could relate to advocates of causality arguing that to be genuinely scientific, one must adopt causality as a scientific method (Hekman, 1979). Brodbeck (1968) adds to this debate by claiming that causal analysis is an inappropriate methodology for the social sciences discipline and the study of human behaviour. Thus, it could be suggested that 'causal explanation' concerns the interpretive understanding of social action rather than external forces implied upon the individual (Clarke et al., 2016).

An example of this theory is discussed by Durkheim (1952) and Douglas (1967), who were very much working within the Weberian tradition. Douglas (1967) demonstrated that an individual's interpretation of an incident, such as suicide, differs from the abstractions that may occur in a more comprehensive social structure. Accordingly, this theory requires exploring the varied factors that may influence where and when specific interpretations of human action are maintained and developed (Clarke et al., 2016). Although Weber (1947) influences social inquiry and the current thesis, they are not confined by this approach. Despite these arguments, it is accepted that Weber (1947) has heavily influenced anthropological research investigating the meaning and understanding of culture embedded in specific social and cultural contexts.

To summarise, Weber's (1947) verstehen position states that: 'social action is distinguished from behaviour. In addition, action, which is directed towards inanimate objects, does not qualify. Action is only social if it takes account of the behaviour of someone else and further action involves more than mere contact with individuals. Furthermore, according to Weber (1947) being jostled by people in a crowded department store does not constitute social action. The action of a social character is confined to incidents where the actor's case is meaningfully orientated to others. In short, this thesis adopts the position that behaviour that is intentional and oriented towards the behaviour of other human beings qualifies as social behaviour (Tucker, 2016).

Employing this theory, "the thoughts constructed by the social scientist to grasp this social reality have to be founded upon the thought objects constructed by the common sense thinking of people living their daily life within the social world" (Shutz, 1962, p.59). Owing to this concept, this thesis approach to investigation within the participant interviews analyses the specific social phenomena of online CSEM offending by exploring the cultural factors, values and thinking of participants in this study.

### 3.7. Inductive and deductive perspectives

The initial qualitative study uses an inductive approach to datum theory with a constructionist ontological position and an interpretivist epistemological stance. In addition, the second part of this study, which employs quantitative data from the IWF, adopts an abductive reasoning approach. It has been suggested that abductive reasoning plays a part in qualitative data analysis, primarily in identifying themes, codes and categories and is not restricted to any particular methodology (Liscomb, 2012). Nevertheless, it should be noted that mixed methods research also considers inductive and deductive perspectives and reasoning (Watkins, 2017; Watkins & Gioa, 2015).

Creswell (2015), Tashakkori & Cresswell (2007) and Tashakkori & Teddlie (1998) suggest that mixed methods consider both inductive and deductive perspectives collectively, while a single-method approach may not satisfactorily answer the research question. That being so, It is generally accepted that although qualitative research leans towards an inductive-subjective contextual approach, quantitative research emphasises a deductive approach, although these methods are not absolute (Morgan, 2007).

Subsequently, deductive reasoning suggests that using this method in the research process is used to test, confirm or refute a theory (Richard & Unrau, 2018).

To support the current research approach, Watkins & Gioaia (2015) argue that qualitative data can be used to build upon a theory that can be evaluated quantitatively, however, this stance appears to be at odds with some arguments in a social science context. For example, Popper (2002, p.143) claims that "deductive inference is absolute and objective; it is a truth". This theory appears absolute, primarily when one explores Bryman's (2004) process of deduction. Bryman (2004), Fig 3.1, claims that theory begins with what is known about a particular domain, leading to a hypothesis that can be tested empirically, leading to confirmation or rejection of the hypothesis. Clark et al. (2021) also note that not all deductive research projects follow this sequence. Consequently, theory per se can include literature relating to specific topics and knowledge gained from other sources.

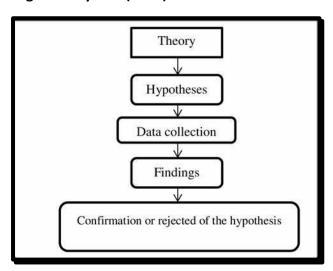


Fig. 3.1. Bryman (2004) The Process of Deduction

The process as highlighted in Fig 3.1. Bryman (2004), should be considered generally as a link between the theory and research. In addition, another approach suggested by Clarke et al. (2021) involves 'abductive reasoning to address the limitations of both inductive and deductive strategies. Abductive reasoning favours a stricter hypothesis-testing process but does not address how researchers should select a theory.

Moreover, abductive reasoning begins with an observation, which commences by explaining the most likely explanation, moving back and forth between the initial observation and the general social aspects of the literature in a process known as dialectical shuttling (Atkinson et al., 2003).

Appropriately, Clarke et al. (2021) argue that abductive reasoning acknowledges that observational conclusions are valid but not entirely guaranteed and may be considered an inference as to the best explanation. In response to Clarke et al.'s (2021) comment, this thesis suggests that although observational conclusions derived from abductive reasoning are valid but not assured, they are relevant to the study outcomes and potential findings. Rapanta (2018) supports this argument by claiming that abductive reasoning is a continuous development process open to revision as new evidence emerges. Furthermore, Walton (2001) claims that abductive reasoning is based on plausibility rather than possibility.

These factors suggest that abductive reasoning is not restricted to any particular methodology and may also play a part in qualitative analysis related explicitly to various other sources, including themes and codes (Liscomb, 2012). Accordingly, given the evidence thus far, abductive reasoning within the quantitative aspect of this thesis is justified. If we turn now to an inductive approach to research, the qualitative aspect of this thesis employs this theory. As Watkins (2023) points out, qualitative data uses inductive reasoning, which begins with observations and finishes with a theory. Crotty (1998, p.32) describes the process of induction in research "whereby a general law is established by accumulating particular instances". Furthermore, Howell (2013) also implies that over many years, the inductive procedure in human and social sciences has indicated accurate scientific statements based on facts encompassing truth, knowledge, and or reality. Accordingly, adopting inductive procedures in a qualitative inquiry ensures conviction in the research findings (Hyde, 2000).

Despite the inductive reasoning chosen for this thesis, it would be remiss to suggest that the theory does not have some criticisms. For example, Crotty (1998, p.32) argues that several philosophers, including Bertrand Russell and Broad, side with Hume in seeing induction as the "weak link in the chain of empiricist science". Moreover, Popper (1994) proposed that knowledge developed through inductive procedures is questionable as the validity of science considers regularity in nature. To support this thesis's argument, Howell (2013) argues that the inductive procedure in natural and social sciences has pointed towards true scientific endeavour for many years.

To summarise, both inductive and deductive approaches have some limitations and benefits conducive to good research. In addition, the abductive approach has also been discussed, which acknowledges that conclusions arising from study observations are plausible but not confident (Clark et al., 2021). While there is consensus that deductive reasoning relates to 'scientific truths', inductive approaches to study reflect upon the implications of the research findings; compared to the opposing principles of deductive reasoning, they are no less valid. Finally, as Howell (1998, p.33) argues, "In search of scientific truth, there is a place for guesswork, intuition, and the follow-up of hunches". This claim by Howell (1998) is valid within the context of this thesis, as qualitative social science investigation is open to some interpretation by scholars but is ultimately strengthened and supported by the arguments and evidence of the research findings.

# 3.8. The case study

The study methodology adopted by the researcher for the qualitative aspect of this work involves a case study. Bryman (2001) describes a case study as an in-depth exploration of a particular case involving a specific community, an organisation, or a person. As Bryman (2001) points out, specific communities or organisations can be explored by using case studies, which in the case of this study involves front-line police officers and civilian staff who work in online CSEM investigations. Aside from this reason, it is prudent to provide other supporting evidence as to why a case study design was chosen by the researcher.

To justify the use of a case study in the research design process the researcher needs to provide a clear argument as to why this method was chosen. Illustrating the use of case study designs, Scapens (2004) posits that case studies within the research process require a defined research question, a well-structured research design and an extensive understanding of the existing literature. Given this stance, the researcher argues that within this study the research question becomes the foundation of social inquiry whilst seeking an extensive understanding of the knowledge surrounding this phenomenon. To further support the use of a case study in the research design, Dul & Hak (2008) suggest that case studies investigate a current phenomenon in a real-world context, more so when the dividing line between the object of the study and its context is unclear. Therefore, as the research design was focused on police officers and staff working in online CSEM investigations, a case study design was deemed to be the most appropriate method for addressing the research question.

However, whilst championing the use of the case study within the research process, it should be noted that there are some criticisms of this concept. Illuminating this, Harrison et al. (2019) point out that the use of case studies may cause some confusion to arise as they are sometimes viewed as both a method and methodology. Moreover, case studies have also been described as a method, a research design, a research strategy and a research approach (Cresswell, 2014; Yin, 2014). However, despite the confusion arising from this, Mills (2014) clarifies this ambiguity by suggesting that methodology is a lens from which the researcher makes decisions about the research process and how the research will subsequently develop. As such, the use of the case study within the research process of this study allows for a greater exploration of the lived experience of police officers investigating online CSEM offending, thereby facilitating a deeper understanding of knowledge and meaning.

Once the case has been selected, one must select a research method to collect the data, however, some caution should be noted when discussing case studies within the research process. For example, Clark et al. (2021), argue that a case study is often wrongly referred to as a method. In that case, exploring the case study concept within the research process is concerned with the complex nature of the case (Stake, 1995). As Holt et al. (2021) note, case studies may involve single organisations, such as Burawoy's (1982) study on factory workers and Holdaway's (1982) study on a single police service.

Using Yin's (2009) theory on the differences in case types, Yin (2009), Table 3.2. describes the five case study types typically used within the research process. Subsequently, the case study within this study takes a qualitative approach with a medium sample size of 9 police officers and 2 civilian investigators in a large police force based in England.

#### Table 3.2. Yin (2009). Types of Case Studies Used in the Research Process

#### **Types of Case Studies**

\_\_\_\_\_

**The Critical Case Study** – Beginning with a well-developed theory, this case allows the researcher a better understanding of what a hypothesis will and will not hold.

The Extreme Case-Commonly used in clinical studies.

**The Representative or Typical Case**-The objective is to capture the circumstances and conditions of an everyday or ordinary situation.

**The Revelatory** -Allows researchers to observe and analyse a phenomenon previously inaccessible to scientists.

**The Longitudinal Case**- Allows the researcher to investigate on two or more occasions.

Using Yin's (2009) approach, this thesis has adopted a 'Representative' or 'Typical' case study approach. Yin (2009) claims that a case study may be selected not because it is unusual or extreme but because it represents a broader category that will provide an appropriate context for answering specific research questions. In this case, a representative approach allows the researcher to investigate and capture the real-life experiences of the participants related to their working practice and knowledge. In addition, Bryman (2004) argues that a representative or 'typical case' focuses on capturing the conditions and circumstances of a situation, which illustrates a much broader category of which it is a member. Thereby, the case study approach in the research design, in this case, is considered a prerequisite for contributing improved theories in the research process (Ridder, 2017).

Case study work is prevalent within social research and many other disciplines, such as science and education (Harrison et al., 2017). Moreover, social scientists have used case studies to investigate social and cultural aspects of individuals' worlds to gain insight into how they attribute meaning, construction and understanding to their experiences (Simons, 2009). As it is, this study intends to investigate the knowledge and training of police officers working in frontline CSEM investigations without the need for testing hypotheses. Yet, despite case studies being a popular choice for social science investigation, there are some limitations and criticisms.

Bryman (2004) notes concerns about case studies involving reliability, replicability and validity and researchers playing down the salience of these factors. Moreover, as Bryman (2004) further eludes, how can a case study research's validity or generalisability produce findings that could be applied to other cases? If we look at Holdaway's (1982) study of a singular police force, the findings cannot be generalisable to every police force in England and Wales. In the same vein, the qualitative aspect of this study relates to a large police force in England; however, the researcher clearly states that this position only reflects one police force and is not representative of others within England and Wales.

To counter the criticism of using case studies for social enquiry, Yin (2017) suggests appropriate ways in which they can be used to enhance the rigour of the research process. For example, Yin (2017) suggests that clear definitions of the subject should be explored in depth along with other factors such as the selection of study cases, data preparation, analysis between cases and a process of triangulation and synthesis between cases. In support of this theory, Mcgloin (2008) argues that a fundamental element of the case study is to ensure that it is confirmable, dependable, and transferable. On this basis, the rigour employed by Yin (2017) related to case studies within the research process provides the researcher with 'checks and balances' to what some researchers sometimes see unfairly as a less reliable method of study.

A further critique against using case studies in research is that some scholars see findings as not generalisable. For example, Bryman (2004) claims that it is sometimes suggested that findings within qualitative studies are often restricted due to the small sample sizes, which makes it difficult to know if the findings can be generalised in other settings. As previously noted, Holdaway's (1982) study within one police force does not represent all police forces in England and Wales. Similarly, this thesis argues that the qualitative investigation in this study raises specific issues and investigations related to police CSEM training overall. Subsequently, as Brymam (2004) argues, individuals interviewed in case studies are not meant to be representative of a population but a generalised theory.

Despite this claim, generalisability within qualitative inquiry may adopt what Williams (2000) refers to as moderatum generalisation, in which the aspects of the research group can be viewed as a more comprehensive set of 'recognisable features. Moreover, as Bryman (2004) argues, when generating findings related to a particular group, the researcher may often compare the findings of other research involving comparable groups. Because of this, comparative research can be applied to numerous situations where the researcher can portray the importance of differing patterns of experience of the individuals (Penn et al., 1994).

Further arguments against the generalisability of qualitative inquiry have their foundations embedded in the ideology of empirical and statistical generalisability (Maxwell & Chimiel, 2014). Moreover, as Braun & Clarke (2022, p.143) claim, in academic literature, some qualitative studies openly apologise for the lack of generalisability in their analysis and "In making such apologies, certain norms or ideals around knowledge are evoked and effectively reinstated as the ideal". On this account, it is suggested that these claims appear to reflect the preconception of qualitative study instead of quantitative inquiry, which argues that qualitative research lacks transparency within the research process.

These claims support the argument that when employing case studies within the qualitative research process, the researcher should not downplay the importance of reliability, replicability and validity. In this instance, Clarke et al. (2022) argue that the primary concern in using a case study is how well the data supports the researcher's theories and arguments. Ergo, the question is not whether the findings can be generalised to a broader audience but how well the researchers generate theory from their findings.

Finally, Yin (2009) calls this inductive approach analytical generalisation, where theory is generated from the research. Subsequently, this approach does not follow a traditional inductive approach, although, as previously stated, case study researchers can often generalise by using the findings from comparable cases (Williams, 2000).

To summarise, employing representative case studies in qualitative research in the context of this study is justified. The arguments for and against generalisability are noted. For instance, the claim made by Braun & Clarke (2014) that some qualitative researchers almost apologise for the lack of generalisability is an interesting point that appears to be the norm in qualitative inquiry. In this thesis, the researcher felt somewhat compelled to note the limitation of the sample size, which was not representative of all police forces in England and Wales, though, this thesis argues that if the same processes were employed using another similar-sized police force using same interview questions, there is a probability that we may generate similar data supporting the original research question.

## 3.9. The study method

As previously noted, further arguments suggest that the research design of a case study needs to ensure methodological rigour, validity, and reliability, which is accepted within the scientific community (Quintão et al., 2020). In addition, Tashakkori & Teddkie (2010) describe the mixed-methods research approach as a broad inquiry into the logic which guides the selection of specific methods, which is guided by relative positions most used by mixed-methods researchers. As this study uses a convergent mixed-methods approach, it is prudent to ask, do case studies have a place in this domain?

Clark et al. (2016) answer this question by arguing that although case studies are often linked to qualitative research, case studies can often involve both quantitive and qualitative mixed-methods research. In addition, Clarke et al. (2016) also claim that mixed methods research is an accepted and widely used approach to social sciences where different methods, using the strengths of quantitative and qualitative ideas, complement the research process. Subsequently, this chapter will focus on the strengths of using a mixed-methods convergent approach and how they are appropriate for the research project.

First, a mixed-methods approach to the research subject allows for different methods to complement one another as the strengths of both qualitative and quantitative methods are amalgamated (Clarke et al., 2022). Still, as Bryman (2010) argues, the differences between qualitative and quantitative research have implications for scientists regarding whether these two concepts can be combined. In answer to this question, Cresswell (2015) claims that mixed-method research considers both inductive and deductive reasoning collectively and individually; a single investigation method may not fully answer the research question. Moreover, as Watkins (2023) also adds, mixed-methods research allows the researcher to extend their knowledge and understanding of the data beyond the capabilities of a single-method study. Hence, mixed methods enable the researcher to thoroughly understand the research problem (Cresswell & Plano Clark, 2007).

While the arguments for employing a mixed-method approach to the research problem have been noted, understanding the various research approaches to this method is required. For example, mixed-method research, as in this thesis, may sometimes use secondary data from other sources. However, It should be noted that there is a distinction between secondary and primary data in the research process where primary data are original quantitative or qualitative data, while secondary data are not new and undergo a process of secondary analysis (Watkins, 2023). Therefore, using secondary data is a reliable way to answer new and existing research questions (Corti et al., 2019).

One of the significant advantages of using secondary data is the wide breadth of data available to the researcher. Clarifying this, Boslaugh (2007) highlights the advantages of using secondary data by pointing out that the data set already exists, saving time by eliminating the need to produce the data. In addition, Boslaugh (2007) claims that there is a wide breadth of secondary data from many sources in all resources. Finally, the third advantage of using secondary data is that the data collection process has already undergone a rigorous process using larger study sets, which is beneficial for small-scale studies such as the current thesis.

As a consequence, using secondary data from the IWF is justified and appropriate for the study's aims. While the advantages of using a mixed-methods approach have been noted, several other designs may be used. Fig 3.2, Watkins (2023) outlines the three main mixed-method approach designs. In the case of this study, this thesis has employed a convergent design based on the aims of this study.

Fig 3.2. (Watkins (2023) illustrates that qualitative and quantitative data are gathered within a similar time frame in the convergent design, sometimes called a concurrent design. Moreover, as Arnult & Fetters (2011) suggest, an interactive approach is used during this time frame, which influences changes in the data collection procedure where, for example, the quantitative findings may influence the focus of the collected qualitative data or vice versa. In addition, more commonly, qualitative, and quantitative data collection may co-occur, whilst analysis for integration begins after the data collection phase has begun or been completed (Fetters et al., 2013). Thus, the convergent design allows two data forms to be analysed and merged rigorously and soundly, encompassing the breadth and depth of a particular phenomenon (Cresswell, 2015).

It is established that qualitative data can be used to build a theory that can be tested quantitatively (Grinnel & Unrau, 2010). Nevertheless, prioritising mixed-methods research's quantitative and qualitative phases will influence this factor. For example, as used in this thesis, prioritising qualitative data first and developing a conceptual framework is the primary goal of using this method. As Watkins (2023) argues, using the qualitative aspect of the research first allows the researcher to build a preliminary conceptual framework to assess a theory in a later phase of the project. In this case, the primary research question asks, is police training and knowledge keeping pace with technology-driven changes in online child sexual exploitation offending? Due to this, using secondary data in this instance will help to answer the research question and generate a theory.

As with any research design, a convergent mixed-method design should follow a specific direction. For example, Fig 3.2 (Watkins, 2023) demonstrates the pathway which a convergent design using new or secondary data should follow. As one can see, the process can be interchangeable, where either qualitative or quantitative data can be used first. In addition, the two data sources remain separate until they are ready to be compared or merged. The final stage of this process involves analysing the data.

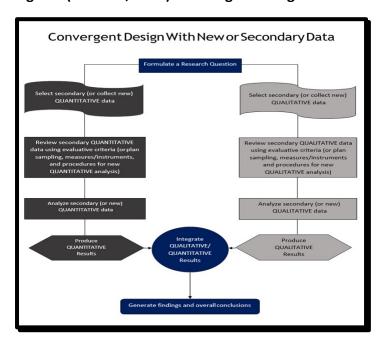


Fig 3.2. (Watkins, 2023). Convergent Design with New or Secondary Data.

According to Creswell & Plano Clark (2018), there are three steps when generating the results from a convergent mixed-methods approach, 'side-by-side, comparison, data transformation, and merging both data sets'. For this thesis, a data transformation approach was adopted as this was deemed the most appropriate analysis for the study. Cresswell et al. (2004) and de Block & Viz (2018) argue that data transformation allows both data sets to be transformed in a manner that enables the researcher to analyse in depth the context in which the data were produced. On these grounds, this thesis has taken a more grounded approach to theory when analysing the quantitative secondary data, as the research aims to gain a deeper understanding of the effects of technology related to online CSEM offending.

To achieve this goal, it was essential for the researcher to interpret the secondary quantitative data using content analysis to analyse the findings. As will be discussed in Chapter 5, the IWF data encompasses various subjects related to online CSEM offending, yet some of these subject areas were unrelated to the research question. Appropriately, a thematic assessment was conducted on the primary themes of importance to the research question.

These themes included the rise in self-generated images of children, the changes and possible causes in children's ages related to CSEM offending, the online risk to younger children sharing images, the changes in online technology and the risk to children, the technology most used by children to share images, and the rise of live-streaming offences.

#### 3.10. The social science interview

This thesis has employed semi-structured interviews (SSI) with police detectives and civilian investigators employed in online CSEM investigations. Semi-structured interviews within the police environment have been used extensively over many years. Illustrating this, Schreuders et al. (2018) conducted a large-scale study of a significant police force related to needs assessment using semi-structured interviews. Evans et al. (2013) used SSI with police officers to investigate their experiences of trauma aftercare. In addition, McClean & Marshall (2010) implement semi-structured interviews in their work on police officers' perspectives on mental health. For this reason, Jamshed (2014) posits that the interview process is the most widely used method in qualitative research. Hence, semi-structured interviews are appropriate for social inquiry within the policing environment.

Brinkman (2018) describes the interview process as an interaction where the researchers ask questions about someone's life, experiences, opinions, and views about a particular subject. Moreover, social science interviews enable individuals to narrate in their own words how they understand and make sense of the world around them (Knott et al., 2022). Nevertheless, as semi-structured social science interviews employ open, closed, and follow-up questions, they may enter unforeseen territory (Adams, 2015). Thus, interviewers must carefully consider their position in this interaction and be knowledgeable and sensitive to the subject area.

That being so, the researcher was fortunate to be able to avail of their previous experience as a CSEM investigator when dealing with such emotive content by careful consideration of appropriate questioning skills.

The interviewer must also acknowledge the power balance between themselves and the participants in the SSI process. Addressing this, Braun & Clarke (2014) suggest that the relationship between the interviewer and interviewee is usually conceived as a hierarchical one. Yet, a counterargument would contend that control within the interview process is not an existing position but is achieved between the interviewer and interviewee (Russell, 1999). Other work by Nunkoosing (2005) approaches the problem of power imbalance during the interview process by arguing that power is always present in everyday transactions between individuals and within the interview process, where the interviewer and interviewee continually strive to deescalate each other's authority. In this event, the evidence thus far would suggest that the role of the interviewer within the SSI process requires a degree of tact, empathy and understanding of the subject matter.

Braun & Clarke (2014) discuss the issues of the societal positions of the interviewer and interviewee, which adds another dimension to the power relationship. This thesis has used SSI with police officers and civilian investigators in online CSEM investigations. As mentioned, the researcher in this study is a retired police officer who has previously worked for many years in this environment. In this context, it is reasonable to suggest that, in this case, the power balance between the interviewer and the interviewee was equal. Moreover, Odenahl & Shaw (2002) discuss the issues of power relationships between the interviewer and interviewee when the researcher has a less equal footing. In this case, the researcher must be meticulous not to let the participants control the interview process.

The SSI method is appropriate for mixed methods study and is a valuable supplement to other approaches (Adams, 2015). This thesis explores secondary data from the IWF, which helps support the interview findings, which cannot be achieved alone by a singular set of interviews. In addition, data from the SSI have previously been used to develop quantitative instruments in the research process, such as content analysis derived from qualitative inquiry used in constructing questionnaires (MaIntosh & Morse, 2015).

It is accepted that this thesis has not used the SSI to create or develop questionnaires or Likert scales but has instead built upon the existing data from the interviews and literature review. In this regard, this thesis uses the interview process to expand on knowledge through a socially constructed narrative.

The SSI method often requires participants to talk about personal issues and sensitive questions, which may become a source of anxiety later in the interview. Also, Braun & Clarke (2006) discuss how to recognise and acknowledge participant distress during the interview process when discussing these sensitive issues. These issues alone suggest that the interview process is not only a socially planned constructed occurrence but also a complex one. The phenomenon of socially constructed knowledge is essential to the everyday understanding that conveys daily life, affecting social relationships and understanding different phenomena (Wiley, 1996). To this end, the social science interview can be described as a delicate balance between the needs of the interviewer and, foremost, the interviewee.

Despite social science interviews being a favoured method amongst qualitative researchers, they are not without some criticism. According to Clarke et al. (2016), qualitative interviews have sometimes been accused of being subjective and difficult to generalise and replicate. The accusation of subjectiveness related to the social science interview stems from the argument that truth is seen as a subjective reality that is experienced in different ways by individuals (Vishenvsky & Beanlands, 2004). Moreover, due to the unstructured nature of the SSI subjectiveness, Collins (1992, p.182) posits that "the entire qualitative research process is biased by implicit assumptions, interest's world view, prejudices, and one sightedness by the researcher". Given this, researchers should be aware of the possible concerns related to subjectivity, the generalisation of findings and prominent ideologies of the researcher in mainstream thinking (Diefenbach, 2009).

The charges against the social science interviews may seem plausible compared to the arguments of 'objective' quantitative inquiry; however, the crucial distinction between both approaches lies within the researcher's attributes. For example, as Hertz (1997) claims, the researcher's perspectives strongly influence the research process and theoretical position, which will affect and determine the research approach and interpretation of the data.

However, as Pyett (2003) argues, although the researcher's interpretation may be more valid than the participant's, they are different and equally valid perspectives. Duly, as Pyett (2003) claims, the researcher's goal is not to distinguish between reliable and unreliable participants but to apply sociological theories and contextual information to understand information beyond the interviewee's perspectives.

### 3.11. The sample

This study has used convenience sampling as the primary approach. Convenience sampling has been described as a type of non-probability sampling where members of the target population meet specific criteria, are readily accessible and are available at a given time (Etikan et al., 2016). As a result, this study has chosen convenience sampling as the participants are often selected around a specific location, such as a police unit working within a police station. Consequently, convenience sampling related to qualitative research depends on the participants' motivation, which may be contingent upon their interest in the subject matter and their wish to express opinions and points of view (Stratton, 2021).

The sample cohort was comprised of twelve initial participants as follows:

- Online sexual crime unit Detectives (n-7)
- Detective Constables from CID (n-3)
- Civilian Investigators within online sexual crimes Unit (n-2).

It should be noted that one interview within the online sexual crime unit cohort was unused as the recording device failed. Participants were recruited via emails sent by the researcher to senior leadership within the relevant department. In addition, invitation letters were attached to the emails outlining the study's nature and the researcher's university's contact details. The initial intake for the study was slow to begin, so a further email was sent to all qualifying staff and officers by the head of the department. No senior managers offered to participate in the study, however, several detective constables and civilian staff agreed to participate. Overall, the participant cohort was well represented by frontline workers investigating online CSEM with 11 used within the study.

Notably, the number of participants, although, medium in size merely a snapshot of one police unit within a large police force and does not represent all police forces in England and Wales.

To summarise, 12 participants participated in the study, resulting in 11 transcripts due to the failure of the recording device on one interview. Notably, officers and staff working in online CSEM investigations are the primary focus of this work. Despite this, officers within the CID departments were also included as they investigated online CSEM crimes.

The researcher had initially expected more CID participants to come forward along with senior leadership; however, this was not the case. Ideally, it would have been beneficial to have at least four CID participants in total to provide a broader picture and comparison of their experience and knowledge of online CSEM offending, digital and social media. Additionally, the researcher had anticipated that at least two senior officers who worked within the online sexual crimes unit would have provided some input regarding their experience of knowledge and learning from a managerial perspective, however, this did not come to fruition. Suffice it to say, from working in a similar background, the researcher understood the reasons behind this reluctance due to the time constraints of the interview process and the often-heavy caseload and managerial duties of the officers. Nevertheless, the overall cohort of participants did provide a realistic sample of frontline workers involved in online CSEM investigation.

#### 3.12. Coding and analysing the data

In this thesis, the interview transcription process was conducted at the researcher's home due to Covid-19 restrictions. To begin, the digitally recorded interviews were electronically transcribed by the University of Nottingham's secure transcription service. Whilst this software is extremely useful, it captures all spoken text in a continuous format where spoken words are often misrepresented. As such, the researcher in this case must listen to the recordings and check the text created by the software to ensure an accurate representation of the participant interview. During this process, the researcher checked the automated transcription by listening to the recordings of the participant interviews and editing them as required onto a Word document. The researcher then anonymised the transcripts which were then saved onto a Microsoft Word Document on the University of Nottingham One-Drive. Finally, the digital recording device used by the researcher was formatted after transferring the interview data to a secure, password-protected university laptop.

As this thesis has used two separate data collection methods, it is crucial to differentiate between quantitative and qualitative approaches. Goertzen (2017) argues that, in its most basic terms, quantitative research methods are used to collect and analyse data that is constructed and represented numerically.

Additionally, Goertzen (2017) also claims that because quantitative data focuses on data that can be measured, it is also effective at answering an open question on a particular situation and uncovering behaviours and trends. On the other hand, qualitative data involves a systematic and rigorous approach to answering a research question and takes the form of words, text, or images (Seers, 2012). Nevertheless, despite the differences in qualitative and quantitative approaches to research, the data require coding in a structured and rigorous manner.

According to Bryman (2010), coding data is a significant stage in the quantitative research process. Also, Bryman & Cramer (2011) discuss the three principles of coding data: the categories generated must not overlap; the list of categories must be complete and cover all possibilities and there must be clear rules about how codes should be applied. In addition, the data are sometimes re-coded to enable the creation of new variables. Due to this, the thesis has used secondary quantitative data from the IWF where the data has been reinterpreted to support the claims within this thesis related to the online risk to younger children and other factors.

Coding the data is a crucial factor in the research process. Braun & Clarke (2022, p.55) describe coding as a "subjective process shaped by what we bring to it", "coding is a process of interpretation or meaning, and researchers' subjectivity fuels this process". Moreover, qualitative data coding can involve different analytical methods; however, as this thesis has adopted TA, complete coding has been used. Notably Table 3.3. (Braun & Clarke, 2014) demonstrates the process of coding using TA. According to Braun & Clarke (2022), complete coding aims to identify everything relevant to answering the research question within the entire data set. In addition, complete coding allows the researcher to analyse all the data. Only later does the process become more selective, where codes identify a feature of the data relevant to addressing the research question.

Table 3.3 (Braun & Clarke, 2014). Stages of Coding and Analysis Used in Thematic Analysis

Thematic Analysis

1. Transcription

2. Reading and familiarisation; taking note of items of potential interest

3. Coding-complete coding across the entire data set

4. Searching for themes

How we code the data is an essential factor, and the researcher faces a wide array of possibilities, including specialist software such as CAQDAS and Nvivo. , Nevertheless, as Basit (2003,p.143) points out, "The choice will depend on the size of the project, the funds and time available, and the inclination and expertise of the researcher". In response to this conundrum, this thesis has also adopted a method of 'tabletop' literal spatial arrangement of coded and categorised data. This decision was based on certain factors related to the practicalities of the data sets and the researcher's experience as a qualitative social scientist.

Saldaña (2021, p.295) argues that "Physically touching the data" and "physically moving the categories in multiple arrangements" assists the researcher in "discovering and understanding such organisational concepts as hierarchy, process, interrelationships, theming, causation and structure". Yet despite this stance, there are some critiques against coding per se, which involve philosophical and methodological concepts. To illustrate this, some scholars argue that coding is reductionist and objective. Saldaña (2021) answers these issues by claiming that coding is what the researchers perceive it to be and is designed to generate discovery.

In addition, for the researcher, "Assigning symbolic meaning or codes to data is an act of personal signature" (Saldaña, 2021, p.23). To summarise, coding the data generates specific themes and categories unique to the researcher, focusing on lived experience, behaviours, recurring phrases, and incidents.

As demonstrated in Table 3.3., by Braun & Clarke (2014), TA involves a series of stages: the researcher immerses themselves in the data; looking for meaning and patterns; generating initial codes and organising them into meaningful groups; searching for themes where the researcher considers how different codes may fit into broader themes; reviewing and refining the themes; defining and naming the themes; identifying central ideas in each theme and finally, producing a written report on the findings (Braun & Clarke, 2014). Due to this, TA is a valid approach to qualitative inquiry where researchers can identify ideas across interview data sets in that what is real is socially constructed (Riger & Sigurnvindottir (2016).

A constructionist thematic analysis (TA) (Braun & Clarke, 2006) was adopted when coding the qualitative and quantitative data. Constructionist TA enables the researcher to focus on how subjects are constructed and how these accounts construct the world. While traditionally associated with qualitative research, TA in all its forms is a flexible tool where coding develops labels and their applications to aspects of relevant data (Braun & Clarke, 2014). Also, according to Joffe (2011), TA helps to facilitate the acquisition of knowledge and meaning by providing the foundations for establishing a valid model of human interaction, thinking, emotions and behaviours. With this in mind, TA was chosen by the researcher as the most appropriate method of analysing and coding the data from both qualitative and quantitative data sets.

As TA is primarily associated with qualitative inquiry alone, this chapter requires an argument for applying this method to the secondary quantitative data. In support of using TA to code both data sets within this thesis, it is crucial to recognise that the secondary IWF data is not purely numerical. Although the IWF data use numerical statistics, they are supported by various themes associated with the numerical data. For example, the theme of live-steam abuse and numerical data for the period analysed are discussed within the secondary IWF data. It is in response to this data that this thesis has employed TA related to the most relevant themes alongside the numerical data.

Under the circumstances, it is acceptable for researchers embedded in several theoretical frameworks to employ thematic analytical methods to try and make sense of technologically rich environments (Ozuem et al., 2022).

To further support the theory of using TA within quantitative data sets, McQueen & Namey (2012) argue that researchers may choose to measure qualitative data sets by employing qualitative methods. Furthermore, as Boyatzi (1998) noted, using thematic analysis to link qualitative and quantitative research can add more validity to both data types. Also, Franzosi (2012) argues that researchers would employ quantitative approaches when more extensive bodies of data are to be analysed. On this account, a reasoned argument exists for applying TA when using numerical data in a specific context.

Yet, caution should be addressed despite the proactive argument for researchers employing TA within data analysis. For example, Franzosi (2012) noted that larger bodies of text requiring analysis might contribute to researchers adopting purely quantitative approaches rather than exploring other methods. Moreover, using a purely quantitative approach in this context could suggest that during the analysis process, the researcher may not fully understand the nature of the data, which is necessary for social science research (Ozuem et al., 2022). Denzin & Lincoln (2018) argue that applying TA to a stringent quantitative paradigmatic approach may result in a narrow view that constrains the framework-driven process, often tendered using a qualitative approach. Appropriately, TA is seen as an accessible process to a broader audience and an appropriate method for participatory approaches where the participants play a role in helping to analyse the data they generate (Braun & Clarke, 2014).

As Creswell & Poth (2016) note, there are five qualitative design approaches to the investigation: Narrative Research; Phenomenological Research; Grounded Theory Research; Ethnographic Research and Case Studies. Despite the differences in these designs, they are all similar in some respects in that all involve the researchers going out into various settings to gather data. As Katz (2015) points out, qualitative fieldwork should incorporate four aspects: Representativeness; Reactivity; Reliability and Replicability. The main points that should be taken away from Katz's (2015) rhetoric should be those relating to reliability and replicability.

It is generally accepted that the methods chosen for generating knowledge are often associated with the researchers' standpoint and background through reflexivity; however, despite this claim, fieldwork should promote inter-observer reliability, which allows others to test the reliability, allowing different observers to have the capacity to identify similar evidence (Ceccato, 2022). As a result, during the fieldwork phase of this thesis, the preliminary data analysis involved the researcher listening to the participant's recorded interviews.

As with other aspects of the research process, trustworthiness is considered the appropriate criterion to ensure reliability in evaluating qualitative studies when analysing textual interview data analysis. For example, Gruba & Lincoln (1989) suggest that researchers employ four criteria during this process: credibility; transferability; dependability, and conformability. Following these criteria allows for prolonged engagement, member checks, and the ability of the findings to be transferred to other contexts to ensure the process is outlined in detail to facilitate replication and ensure the study minimises research bias by acknowledging the researcher's predispositions (Maher et al., 2018). Subsequently, dealing with large amounts of qualitative interview data can be a challenging process for the researcher as they are tasked with interpreting the data considering both the theoretical and practicalities of the process.

# 3.13. Ethics and reflexivity

Ethics plays an essential role like any research process within the social sciences, yet ethical problems within qualitative studies differ from those in quantitative research. For example, Orb et al. (2001) highlight the potential conflicts in qualitative research regarding how the researcher gains access to organisations and participants. In addition, Bryman (2004, p.130) discusses the ethics of social research by claiming that "Ethical issues cannot be ignored, as they relate directly to the integrity of a piece of research and the disciplines involved". In this context, researching online CSEM offending is a sensitive issue in which the participant's and the researchers' welfare is paramount.

Police officers and civilian staff working in online CSEM investigations are vulnerable to stress caused by the nature of their role and the heavy caseload of their work (Wright et al., 2006). In addition, Violanti & Gehrke (2004) also highlight the thematic nature of police officers who are exposed to child abuse investigations as part of their role.

Earlier work by Deiner & Crandall (1978) suggests four main areas to consider when working with vulnerable interviewees, which are a risk of harm to the participant, whether there is a lack of informed consent, whether there is a breach of privacy and whether deception is involved. In that sense, the researcher should note extreme caution when engaging with participants who may be deemed vulnerable.

Some could view harm to participants as subjective, however, harm can include loss of self-esteem, stress, and emotional, psychological, and physical harm. A well-known example of participant harm noted by numerous scholars over the years can be seen in Milgram (1963). In addition, there have been many studies over the years involving police officers and staff working in child abuse investigations and other stressful police occupations where ethical considerations have been followed. Notably, ethical approval by the university or organisation is always a prerequisite where there is a risk of harm to the participants.

Before the interviews commenced, the interviewer informed the participants that if they became upset during the interview, they could stop the process and resume later or withdraw completely. In addition, the researcher could signpost the interviewee to support and welfare services if required, however; although some interviews did raise several welfare issues, there was no requirement to halt any interviews or refer staff to support services. It should be mentioned that some unused material from the interviews in this study related to welfare was used to publish a needs assessment with the respective police organisation.

In addition to the interviewee's welfare and well-being during the interview process, it is vital to recognise the emotional safeguarding of the interviewer, especially when dealing with sensitive subjects such as child abuse. Yet, the emotional safety of interviewers is not a new concept despite the plethora of academic evidence related to participant well-being during the interview process. Earlier work by Brannen (1988) argues that researchers who are trusted with the confidence of interviewees should be protected by safeguards. In addition, Brannen (1988) also highlights the role of supervision in occupations where counsellors are often exposed to the rigours of emotive subjects. Consequently, the emotional safety and well-being of the interviewer are also paramount during the research process.

Notably, the emotional well-being and resilience of the interviewer were factors within the ethics process, and amendments were made to address this. For example, the researcher ensured that along with signposting support services for the interviewees, they were also aware of the emotional intervention provided by the University of Nottingham Student Services and the host police organisation, where the researcher was also a Police Support Volunteer. Moreover, despite safeguarding interventions within the ethics process, it is accepted that there is always some degree of risk to both the participant and interviewer within the research process. Considering this, employing strategies that include building rapport, self-disclosure, sensitivity and reciprocity can help within the interview process for both the interviewer and participants (Elmir et al., 2011).

In addition to self-care, interviewees must provide informed consent during the research process. As Bryman (2004) notes, informed consent is a vigorously debated topic within social research. Nonetheless, most of these discussions relate to what is sometimes called disguised or covert observations. This thesis did not use covert means, so this was not an issue. However, social researchers should approach ethical considerations from various standpoints to avoid ethical transgression. For instance, Clarke et al. (2021) discuss some ethical approaches, which include universalism, situation ethics, deontological and consequentialist ethics. Accordingly, the ethical approach taken by this thesis involves a universalist approach.

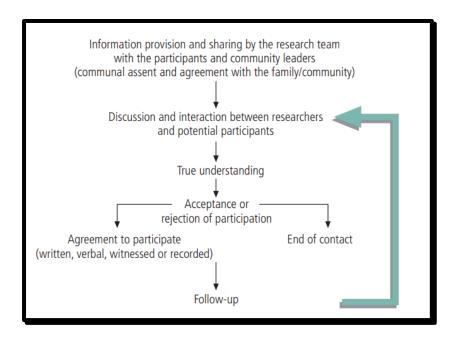
When exploring the theory of universalism within the ethics process, Benhabib (1994, p. 173) states that "All human beings, by virtue of their humanity, are entitled to moral respect from others". Moreover, as Abbott (2023) posits, universalism seeks to formulate a universalism that accounts for both generalised features of what makes us human and the differences in our circumstances and experiences when considering how we treat our fellow human beings. Consequently, the ethical considerations in this study are that no deception or ill-treatment of participants was involved in the research process, nor was any violation of ethical principles.

Illustrating this, some scholars argue that ethical transgressions are sometimes justified. For example, Punch (1994) suggests that withholding certain information from the participant is intrinsic to personal experience and research. Earlier work by Gans (1962) adds that if the researcher is honest with the participant, there is a possibility that they may hide their opinions and attitudes they consider inappropriate, and their narrative will not be an accurate reflection. In addition, Clark et al. (2021) discuss deontological issues within the ethics process where, for example, deceiving participants into not providing informed consent is seen as ethically wrong. Based on this, informed consent within this thesis is an essential ethical consideration.

Clark et al. (2022) describe the process of informed consent as providing the research participants with satisfactory information as needed to make an informed decision regarding whether they wish to participate in the study. Also, Bryman (2004) adds that even if participants have agreed to participate in a study, they should be fully informed about the research process. Fig 3.3. (Bhutta, 2004) outlines a conceptual framework for developing informed consent within the research process.

As one can see, this process allows the research team to provide a complete and transparent overview of the research study and the participants' rights in a manner that can be understood. Additionally, the participant is then provided with information that describes what is expected from them in clear, unambiguous terms. Finally, the last process argues that participants must freely agree to participate in the project, understand all it entails and provide their written consent.

Fig 3.3. (Bhutta, 2004) Conceptual Framework For The Elements and Detriments of the Informed Consent Process.



Likewise, in this thesis, the researcher followed this process in a similar form by providing participants with a completed information sheet and a consent form, which was read by the participants and signed in the presence of the researcher. The researcher used no coercion or covert issues in this study, and the participants were fully appraised of the study and the motivation involved. Moreover, researchers must emphasise the confidential nature of the research process for ethical considerations and as a primary factor in an individual's decision to participate (Bourne & Robson, 2015). Resultantly, as Lee (1993) suggests, by providing confidentiality and anonymity at the outset, there is no reason participants cannot provide frank and honest accounts in their responses during the interview process, even when faced with sensitive topics.

Regarding access to the interview data, only the principal researcher and the two supervisors have access to the anonymised interview transcripts. In addition, all participants were given a pseudonym, and no real names were used during the interview or in any hard copies of documents or published material. Furthermore, no identities of the interviewees were stored on any data storage devices or laptops. Ethical applications were submitted to the University of Nottingham School of Computer Science, and after some amendments, approval was granted to commence the fieldwork.

Fieldwork commenced on 19th August 2020 and was completed on 28th June 2021, resulting in 12 digitally recorded interviews. As previously mentioned, one interview was not saved correctly and is unusable for this thesis. Before the interviews, both the interviewer and the participant reviewed the information sheet. In addition, after reviewing the information sheet and consent forms, the participants signed the consent form in the interviewer's presence and were invited to ask questions. Conducting social science research within the police service can sometimes be problematic. To this end, Wilson et al. (2023) allude to the importance of positive collaboration between academic institutions and police organisations, which is imperative to public safety.

As the researcher is a retired police officer who had worked in a similar environment to the participants, their presence and interest in the working practices of the participants were accepted. Moreover, in their work, Davis (2016) delineates some of the challenges related to conducting research within the police concerning (Brown, 1996) typologies of police 'insiders' and 'outsiders'. Furthermore, as Davis (2016) posits, 'outside' police researchers are incentivised to work collaboratively as part of knowledge exchange, while on the other hand, internal police research is driven by an evidenced-based approach which encourages 'greater analytical capabilities of the 'insiders'.

The acceptance of the researcher by participants within police organisations is difficult, given the nature of the policing environment and sub-culture. Earlier work by Conser (1979) discusses the policing sub-culture, which is unique to this society, where facets are noted, including sub-groups, personal characteristics, behaviours, values, and identity.

Also, Greico et al. (2014) raise the issues of police and researcher relationships, which may challenge the conventional philosophies of law enforcement organisations and research culture. Accordingly, the researcher did not experience any negativity or suspicion from participants, resulting in an open and frank discussion among the interviewees.

## 3.14. Reflexive practice

The study and investigation of child sexual abuse is an emotive subject. Many scholars have debated the health implications of workers and staff investigating online and physical child sexual abuse. To illustrate this point, healthcare professionals working with the police know the adverse effects of exposure to child abuse material and the psychological risks (Tehrani, 2018). Despite this, whilst it is important to understand the negative health effects on police staff, consideration should also be given to the researchers and supervisors who engage in studies in this area.

The following quote from Coles (2006, p.141) sums up the health risks faced by researchers in the area of child abuse, "on the way home from interviewing one participant, I had to stop the car and park up on the edge of the road, I felt nauseous and thought I would vomit, the physical reaction passed, but I remained in my car at the edge of the road, weeping for the little girl who's (abuse) story I had just heard". The emotive words from Cole (2009) highlight the self-care needed for researchers when conducting emotive research. Against this background, it is important to include some thoughts on reflective practice in the context of this study.

Reflexive practice in qualitative research has been described as the degree of influence that the researcher uses either intentionally or unintentionally (Jootun et al., 2009). In addition, Howell (2013) argues that reflexivity involves critical thinking by the researcher about different concepts of oneself within the research process. Because of this, the relationship between the researcher and the research is valid and deserves attention. Accordingly, values and bias can occur at any stage of the research process, where sympathy and affection may emerge, which were not necessarily present at the start (Bryman, 2001).

Subsequently, reflexivity in the research process involves critical thinking about the concepts of oneself throughout the research process (Howell, 2013). On the other hand, reflexivity is essential to this thesis as it highlights the positionality and values of the researcher, which may impact the research process (Walker et al., 2013).

It is claimed that reflexivity within quantitative research is rare due to the philosophical dichotomy between qualitative and quantitative research (Mauther & Doucet, 2003). On the other hand, some would argue that reflexivity is usually associated with qualitative research methods (Walker et al., 2013). Yet, as Ryan & Golden (2006) argue, research decisions are an integral part of the research process; subsequently, reflexivity adds an intuitive understanding of the complex workings that exist in quantitative research. This argument is relevant as this thesis has used a qualitative and quantitative approach that has employed a thematic analysis of both data sets. Furthermore, Clark et al. (2021) argue that reflexivity in this sense is essential as social research often employs a variety of methodological standpoints that do not always agree with each other. In this setting, this thesis argues that reflexivity is essential for both qualitative and quantitative research approaches.

As the researcher is a former police officer working within the role of CSEM investigation, it is appropriate to mention the issues of research bias. According to Pannucci & Wilkins (2010), research bias may occur at any stage during the collection of data, the analysis, and the publication of findings. Moreover, as Smith & Nobel (2014) claim, researchers can bring their own experiences, ideas, prejudices, and personal beliefs to the research process, which, if previously stated, can enhance the rigour and transparency of any possible research bias. Subsequently, reducing bias in the research process enables the researcher and policymakers to scrutinise and evaluate findings when applying the data to practice and policy (Smith & Nobel, 2014).

#### 3.15. Conclusion

This study has evolved and adapted over the previous four years. This work's original concept and ideas were originally related to online police officers' knowledge and training and CSEM offenders and their use and knowledge of digital platforms and social media sites used for offending. Nonetheless, due to the COVID-19 pandemic, the primary ideas for this thesis have been adapted to enable the collection of other suitable data.

As the research progressed, it was evident that options with data collection on the issues of online CSEM offending would focus on the police and the technology industries' responses to the growing concern of illegal online child sexual abuse.

Appropriately, data from one principal technology-focused organisation, the Internet Watch Foundation were explored along with data from Thorn. At the same time, it would have been beneficial to hear the experiences of those who engage in online CSEM offending behaviour and how their use of technology has changed and adapted. Several organisations and charities that work with online CSEM offenders were approached with a view of conducting research in this area. Unfortunately, requests for access to potential participants in these organisations were declined. However, this did not diminish the importance of the data collected in this study or the resultant findings.

Finally, after exploring the methods and methodology of this study, the next logical sequence is to focus on the participant interviews. The participant interviews in this study form the bedrock of the purpose of this study which is to explore the digital and social media knowledge and training of police officers who investigate online CSEM offending. Therefore, Chapter 4 explores the narrative of the interviewees related to their lived experiences investigating online CSEM offences, which is a vital aspect of this study if we are to identify and understand areas for future improvements to working practices.

The next section of this thesis presents the participant interviews with police officers and staff working within online sexual crimes investigation in a major UK police force. The primary themes relate to the online technical knowledge and social media training of police officers and civilian staff working within online sexual crime investigations. While the focus of this thesis is to explore the online training and social media knowledge of police officers, this chapter will also focus on other relevant subjects which underpin the research question. The primary subjects in this chapter include the qualifications and training of officers; role accreditation and image grading training; the current level of officers' training; the experience of knowledge sharing and the impact of police officers' knowledge and changes to online CSEM offending behaviour.

'It would be fair to say that no other cybercrime issue has elicited the degree of anxiety as that over the circulation of sexual images of minors on the internet.'

(Yar & Steinmetz 2019, p.175)

### Chapter 4. The Participant Interviews

#### 4.1. Introduction

For this part of the study, semi-structured interviews were conducted within the confines of police stations in meeting rooms and private offices. The interviews took place with serving detective constables in the online sexual crime unit (n-7), Divisional CID officers (n-3) and civilian investigators (n-2). The interviews were also supported and approved by the senior officer in charge of the department and the research department of the police force in question. No senior line managers above the rank of sergeant volunteered to participate in the study. Even so, despite the lack of senior managers, it is still apparent that police constables are the primary response to cybercrime investigations (Holt et al., 2020). For that reason, the researcher believes the lack of senior officers in the study does not distract from the findings. Notwithstanding, future research in this field would benefit from engagement from senior management and leadership input (Lee et al., 2019).

It is essential to mention that three interviewees were based within a front-line CID (criminal investigations department) unit within the police force explored in this study. The CID traditionally investigates other serious crimes, requiring more investigation skills than front-line police response. It was envisaged that more participants from CID could be sourced to compare their digital and technical knowledge, skills, and experience with those officers working within the online sexual crime unit. As such, the uptake for CID officers was low.

Investigating online sexual crimes is not the usual remit of CID officers compared to colleagues in online sex crime investigations and one probable reason for the low response from CID officers is provided within the interviews by one participant who cites a heavy caseload as a significant issue for detectives working within CID. Although based on nursing staff and not police officers, Hicks (1995) and Hundley et al. (2000) claim that nurses' reluctance to participate in the research included a lack of time, staffing levels and a negative attitude towards the research. One CID interviewee raises this point within the following quote, "I will say for selfish reasons because of staffing levels, CID is far too swamped, we are struggling at the moment, and unless something is done urgently, then they will go under." As a result, it could be suggested that the lack of CID officers' take-up could be due to the high caseloads and ongoing investigations.

To summarise, It is crucial to understand that the themes within this thesis and the narrative from the participants may not represent the experiences and attitudes of staff from other police services who work in online sex crime investigations. For example, different police forces may have similar units, but not all are trained similarly which is why it is important in this study to note these differences. Subsequently, the themes discussed in this chapter are relevant to the research question and include understanding police officers' online digital training and social media knowledge and awareness related to their specialised role.

## 4.2. An overview of the interview questions

Before exploring the narrative from the participants regarding the interviews, it is beneficial for the reader to provide an overview of the interview questions and their rationale. Two sets of interview questions were devised by the author for both CID officers and the online sexual crimes unit participants. As the reader will note, the interview questions are different between the CID officers and their online sexual crimes unit colleagues. The divergence in the interview questions was designed to highlight the differences in the role of the CID officer who investigates CSEM offending along with other serious crimes and their colleagues who routinely investigate CSEM offending.

If we take the online sexual crimes unit interviews first, the questions are directed at both the two civilian investigators and police detectives which comprise the interview cohort:

#### Interview questions for Online Sexual Crimes Unit participants.

- 1. Can you describe your role within the police and tell me if you are a civilian worker or a police officer?
- 2. Can you tell me in broad terms how you receive case referrals regarding Indecent images of children?
- 3. What are the main types of or more common referrals you receive?
- 4. Are you satisfied with the methods of referrals from internet service providers, NCA, and other agencies, and if not why?
- 5. Do you feel that improvements need to be made in how your organisation responds to the referrals and if so what would they be?
- 6. Do you know what referral procedures other organisations such as the NCA use?
- 7. Are you satisfied with the standard of referrals you receive and what is the quality control like?
- 8. Do you feel your training is satisfactory and if not what could you suggest to improve your knowledge?
- 9. Would you feel that you would benefit from having some working experience with partner organizations such as the NCA?

- 10. What do you enjoy most about your work and what do you dislike?
- 11. Do you feel that your role is hampered or slowed down by anything such as any procedures which could be streamlined?
- 12. Would you welcome any new ideas or suggestions from either your own or other organisations which would improve your working practice?
- 13. Is there anything else you would like to add?

As with any set of interview questions, there must be a degree of motivation to enable the researcher to gain an understanding of the participant's lived experience within a particular domain. For example, Roberts (2020) suggests that interview questions used by researchers should be appropriate and can support the goal of obtaining detailed answers to the specific research question. In this case, the researcher wished to discover the standard of online digital knowledge and training of police officers and staff working in online CSEM investigations.

As one can see, the first question asks the participants if they are police officers or civilian staff members. It is important to make this distinction as even though they may carry out similar duties, the training and knowledge of civilian investigators may differ from their policing colleagues. Notably, the first set of questions, 2-7 relate to the referral systems for CSEM cases which the officers would then be allocated for investigation. This area is a vital aspect of addressing the initial research question as it is a method of gauging the officer's overall knowledge and understanding as to how and why online CSEM referrals are made. For example, some officers may have differing knowledge of how NCMEC and other agencies such as the National Crime Agency identify CSEM material and the technology used to remove and report illegal content. Subsequently, asking questions related to the referral procedure provides an opportunity to explore the level of knowledge and training of these officers regarding the technology used to identify and remove illegal online content.

Notably, questions 8 and 9 are significant as they directly address the standard of training the officers have received related to their roles and also the collaborative working practices with other partner organisations including the NCA. The final questions, 10-13 are related to job satisfaction and any other matters that the participant would like to add. These questions are no less important as the researcher must allow the participants a voice outside of the principal aims of the study which may open up further responses to the research question which may be valid. Illustrating this, Polit & Beck (2010) and Galletta (2013) posit that enabling reciprocity between the interviewer and participants enables the interviewer to improvise follow-up questions and also allows for the participant's verbal expression. Therefore, as Raworth et al. (2012) suggest, at the end of semi-structured interviews, it is always useful to ask the interviewees if they have any questions they would like to add, allowing for some degree of flexibility within the participant's responses.

The next set of interview questions was designed for the CID participants. Notably, these questions were different from the online sexual crimes unit interviewees which is designed to highlight any differences in their roles, training and responsibilities. This is an important facet of the interview process as the CID officers in this study investigated CSEM offences along with other serious crimes including sexual assaults and rape offences.

#### Interview questions for CID participants

- 1. Can you describe your role within the Police and if you are a civilian worker or a police officer?
- 2. Can you tell me in broad terms how you receive case referrals regarding Indecent images of children?
- 3. Do you understand the methods, platforms and technology used by offenders to access and share indecent images of children?

- 4. Regarding the methods social media sites used by offenders, what are the most significant issues or problems you encounter when investigating offences using digital platforms?
- 5. Do you have any specific training on investigating indecent image offences and if not would you like to improve your knowledge?
- 6. If you have to investigate indecent image offences what parts of the referral system and training could be improved upon?
- 7. Would you welcome any new ideas or suggestions from either your own or other organisations to improve your working practice?
- 8. As a CID officer do you feel that your department should be investigating indecent image offences?
- 9. Does the investigation of indecent images of children have an impact on your other workload?
- 10. Are you comfortable investigating image offences and viewing the images and if you have been affected what support systems are in place and would you use them?
- 11. Do you feel that the online sexual crimes unit or a dedicated department should deal with all indecent image offences rather than CID?
- 12. Finally, is there anything else that you would like to add?

Similar to the questions addressed to the online sexual crime participants, the initial questions, 2-7 are related to knowledge of the referral systems, specific training and knowledge of investigating online CSEM offending, social media awareness and improving knowledge in these areas. Again, these questions similar to the online sexual crime unit interviews were designed to gain relevant responses to the participant's overall training, improvements to knowledge related to their role and collaborative training with partner organisations. However, questions 8-11 are directed towards addressing the differences in the working practices between the CID officers and the staff within the online sexual crimes unit.

As previously mentioned, this difference is an important facet in addressing the initial research question as although CID officers appear to investigate similar offences as their online sexual crimes unit colleagues, the primary difference in their training appears to be a lack of image grading training. Finally, it has been noted that alongside investigating similar offences to their colleagues, CID officers also investigate other serious crimes as part of their duty. The responses to this subject are seen later in this chapter regarding the narrative of some CID participants. To finish this section, the differences in the interview questions for the CID officers and their colleagues in the online sexual crimes unit are valid as they allow for different perspectives despite the similarities of their roles when investigating online CSEM offending.

To begin, the next heading explores the qualifications and training needs of the participants, beginning with those working within the online sexual crimes unit. This section addresses the primary issues regarding the training and qualifications of those officers working within the online sexual crimes unit when compared to CID participants.

## 4.3. The qualifications and training needs related to online CSEM investigations?

Cushion (2018) claims that training plays a resolute role in police officers' skills and development. Whilst this claim may seem justified, the training for police or other organisations is only helpful if it produces the desired effect, outcomes and objectives (Huey, 2018). Nevertheless, most existing studies on this subject are descriptive rather than evaluative and call for more police training research (Aguilar-Moya et al., 2013).

So, it is essential to hear the participants' narratives to gauge how police training and knowledge in online sexual crime investigation can be improved or adapted to meet the changing nature of online offending technology. To begin, the interviewees in this study narrate the training and qualifications required by their police force to enable them to work in online sex crime investigations:

Frank, DC, online sexual crimes unit: So, there is no specific course you have to go on to be in the office. Once you are in the office, you need to be able to identify child abuse images so that you would do a course in identifying child abuse images.

Dan, DC, online sexual crimes unit: No, you just have to be a detective constable, so you do your ICIDP course (detective course).

Eddy, DC, online sexual crimes unit: You need to be ICIDP (Detective course), so you need to be a detective.

(Parenthesis inserted by the researcher)

When exploring the interviewee's narrative, it appears that the primary requisite for investigating CSEM involves having detective status and, in the case of online sexual crime unit staff, being trained to grade indecent images of children. The ICIDP course (Initial Crime Investigators Development Programme) appeared to be a prerequisite for acceptance within front-line detective roles, including online sexual crimes investigation. Furthermore, no training was provided or encouraged for participants by senior line managers regarding online digital platforms, social media knowledge, or awareness. Similarly, interviewees noted other training issues and were asked for their narratives about opportunities for working experience with partner organisations, such as the National Crime Agency (NCA).

Exploring cross-working partnerships, McCarthy & O'Neill (2014) claim that partnerships amongst police organisations are a part of everyday working life, which help to deliver a range of community responses and services. As a result, the interviewees were asked if they would benefit from spending several days with the NCA to see how their organisation worked and if they would benefit from their experience.

Illustrating this, McEwen (2003) suggests that the benefits of working with other organisations provide opportunities for organisational leaders and researchers to draw upon the expertise and empirical knowledge, which can help to develop responses to societal problems. Here, the interviewee's narratives appear favourable when discussing this concept. Interestingly, one interviewee uses an analogy relating to a car production line when discussing inter-agency working:

Eddy, DC, online sexual crimes unit: Working with other agencies, I always look at it as if you work in a car manufacturing plant and you are fitting the windscreen wipers. Your job is affected by the guy who works before you and the job before you, because if you don't understand what his issues are, then you can't do your job properly.

Harry, DC, Divisional CID: The more knowledge and more training officers are given, the better equipped at investigating these kinds of crimes and also (you are) getting the best evidence.

Jennifer, civilian investigator, online sexual crimes unit: I think if you could see what they did on their side, it would probably help us, knowing exactly what they needed and what they needed it for.

While the quotes from some interviewees were positive, other participants were not as enthusiastic about the prospect of work experience with the NCA. On the one hand, some participants welcomed this suggestion, while others highlighted the differences between police and NCA staff. For example, interviewees highlight differences between the police and NCA, primarily relating to their perceived civilian role rather than being police detectives:

Dan, DC, online sexual crimes unit: We are completely different entities, aren't we? The NCA have different powers to us and work in different ways to us, even though they are Home Office agents. The way they work is completely different to a standard police force.

Alan, civilian investigator, online sexual crimes unit: I do not know the background of the NCA staff, but because they are part of the civil service, you could be working in HMRC and then working in the bureau tomorrow, you know it is not the police world, it is a civil service role. On the issues regarding the NCA and their standards image grading training:

Claire, DC, online sexual crimes unit: I think it is down to poor (training); obviously, they are trained like we are trained, but they don't ever get that in the referral section, and they are civilian members of staff that have just been placed in there.

(Parenthesis inserted by the researcher)

Notably, some interviewees held negative views of their counterparts within the NCA. Additionally, some of the interviewees claimed that NCA staff were not police officers but civil servants, which may indicate an attitude of professional hierarchy compared to civilian staff within the NCA. One explanation for this could relate to the robust cultural and organisational makeup within the police, which may lead to challenges in internal changes and planning (Loveday, 2017).

Additionally, Cockcroft (2019) highlights this point further by claiming that every policing organisation and its environment brings with it particular demographic and historical remnants that may impact future organisational challenges.

Upon further analysis of the interviewee's narrative, it could be suggested that some may have stereotypical attitudes towards their counterparts within the NCA by claiming they are "civilians" and "civil servants" instead of police officers. Stereotyping amongst professionals is not new in academic studies and is noted in the literature. For example, in their exploration of professional stereotypes, Bell & Allain (2010) claimed that in professional stereotyping, there are strong intimations concerning power and status, which may result in a so-called 'pecking order' of qualifications, experience and expertise (Jones-Devitt & Smith, 2007). Duly, some participants may have preconceptions about professional qualifications when discussing their counterparts within the NCA.

Despite these participants' claims, earlier work by Lyneet et al. (2001) suggested that shared learning amongst groups effectively reduces interprofessional stereotypes. Moreover, Watkin et al. (2009) highlight the importance of overcoming barriers and cultural differences to enhance practical inter-agency work to improve service delivery and interagency teamwork. But, to achieve this goal, police officers must achieve status within their organisations through education and qualifications, alongside performance management mechanisms and other principles to improve organisational efficiency (Thursfield, 2012).

Proportionally, it is reasonable to understand why some interviewees feel their role as specialist police detectives reflects Jones-Devitt & Smith's (2007) claims of a hierarchy of expertise and experience. Nevertheless, the importance of co-working with collaborative organisations such as the NCA should not be diminished. As Nikolić's (2020) review of the NCA points out, the fight against global crime may only be achieved through well-coordinated, inter-agency cooperation. Hence, inter-agency work experience partner-ships should be encouraged, allowing the NCA and front-line police child abuse investigators to avail of shared skills, experience, and knowledge sharing.

When analysing the interviewee's claims so far, the primary qualifications and training required within the online sexual crime unit are detective status and image grading training. In addition, CID interviewees received similar detective training other than training in grading indecent images. Notably, interviewees in this study come from various backgrounds within the police, including economic crime, safeguarding and CID. Yet, how they learn once they arrive within the unit is essential to understanding police knowledge and training within this field.

While the level of qualifications for online sexual crimes staff is noted, detectives working in CID were also asked about their qualifications and training. Although detectives within the CID investigate some online CSEM offences, their training in online crime sexual crime investigation appears inconsistent with their colleagues in the online sexual crimes unit. That being, the main difference between CID officers and those working within the online sexual crime unit was image grading training and experience.

The Interviewer asked the question to CID officers: *Do you have any specific training on investigating indecent images, and if not, would you like to improve your training?* 

Kelly, DC, divisional CID: I can't think of any specific day where we have been to class to learn about it. It's all been pretty much ad hoc.

Georgina, DC, divisional CID: Sometimes, specific training isn't needed to be able to do it (the job) effectively, but it would definitely help.

Harry, DC, divisional CID: We are not given any training in relation to that. It just kind of comes as you are an investigator; a job will come in, and you investigate in a systematic and common sense sort of way.

(Parenthesis inserted by the researcher)

Although CID officers often deal with a wide range of serious offences, including CSEM, their training appears inconsistent with what is expected from them. Illustrating this, one interviewee uses the term, ad hoc' to describe their training, suggesting that training and knowledge are intermittent at best. On the other hand, another CID participant argues that specific training was not required to do their job effectively when investigating online sexual crimes.

Resultantly, an interviewee cites that being an investigator first is crucial as they will investigate a crime in a "systematic and common-sense manner". Nevertheless, despite this interviewee's claim, online sex crimes differ in their investigational approach to other crimes. For example, many policing challenges within online sexual crime include the legal jurisdiction of countries, Tor networks and the hidden web, and detection and reporting methods (Owen & Savage, 2015; Yar & Steinmetz, 2019).

Within this framework, online sexual crime investigation calls for a structured and formal approach to investigation, knowledge sharing and learning. Responding to this, interviewees in CID were asked what type of online offending behaviour they would usually investigate. Responses included indecent image investigations, grooming and sexualised chat offences, more or less the same offences as their colleagues in the online sexual crime unit.

The interviewer asks CID participants: *Is it only images that you would get? Is it just images you look at in CID?* 

Kelly, DC, divisional CID: We can have indecent sexual abuse images and also grooming offences as well, and then going on to sexual assaults and rapes.

Harry, DC, divisional CID: I think we would deal with (sexualised) chat offences as well because some of the content of chat offences can be quite horrendous as well.

(Parenthesis inserted by the researcher)

Despite the CID interviewees claiming that they investigated most aspects of online sexual crimes, they appear to hold no relevant qualifications or training specific to online CSEM investigation other than having detective status, yet, if we are to understand the priorities of police training, it must rely on internal and external evaluations (Huey, 2018). To this end, this thesis attempts to address this issue by suggesting changes in police training and knowledge to all officers including those in CID who investigate online CSEM offending.

To support the thesis argument, previous work by Mugford, Corey & Benell (2011) claims that the literature on police training lacks empirically supported planning that can be integrated into training and transferring skills and knowledge. Also, Schreuders et al. (2020) argue that many officers policing digital crimes have limited knowledge of technology. Thus, there is a need to explore how training and knowledge are captured and shared within frontline investigation units. Consequently, it is difficult to understand what future changes are required in training and service delivery in online sex investigation without exploring how interviewees in online sexual crime units are trained to conduct their roles. To this end, the next main section explores the training related to the grading of indecent images which is mandatory for officers in this study. In addition, official accreditation is discussed with participants.

#### 4.4. Role accreditation and Image grading training

So far, the thesis has identified that the primary qualification for participants in the study for working in online CSEM investigation is having detective status and image grading training. Regardless, asking interviewees about any recognised official accreditation relating to their role was prudent. Official accreditation within online sexual crimes investigation has been noted previously and is discussed in Chapter 2, the literature review. Yet, despite holding no official accreditation to their role per se, participants highlighted image grading as a principal requirement of their training and an essential part of their role:

Dan, DC, online sexual crimes unit: There should be an amalgamation of skills, we have too many people in our office who have certain skills that others don't have, and I think there needs to be some form of accredited training.

Jennifer, civilian investigator, online sexual crimes unit: I've obviously done my grading course, so I'm a qualified grader, but that's it really.

Frank: DC, online sexual crimes unit: Once you are in the office, you need to be able to identify child abuse images, so you would do a course in the identification of child abuse images.

Eddy, DC, online sexual crimes unit: I don't think I have had any (training) in this specific field of work. What is interesting is that I now deliver the training on ICDP (detective course) for indecent image investigation, which is an improvement as I never got that.

(Parenthesis inserted by the researcher).

Official accreditation by one interviewee is noted, yet despite this, when one explores the knowledge of UK police fraud investigators, they are fully accredited and hold formal qualifications to conduct complex financial investigations (Button et al., 2007; Chave, 2017). All the same, detectives working on online sexual crimes within this study do not have formal accreditation other than being detectives and holding image grading training.

When exploring the image grading training of the participants in this study, there appear to be inconsistencies between the training received by other major UK police forces. To address this issue the author submitted several requests to other police forces intending to conduct further qualitative studies in this area. However, due to various reasons including COVID-19 restrictions, these requests did not come to fruition.

To overcome this barrier, the author applied for freedom of information requests (FOI) from three large police forces in England, Appendices, A, B and C. The rationale for applying for these freedom-of-request applications was to provide some context as to how officers and staff from other police forces in England were trained and qualified in online CSEM investigation. Illustrating this, the first freedom of Information request, Appendix A, (No 01FO1/22/027327 dated 22<sup>nd</sup> December 2022) states that ..." trainers who are trained and accredited in [ image grading ] by the Home Office...are then sanctioned to train other officers". "However, those who receive the secondary training are not accredited the same way as those trained by the Home Office".

Similarly, the second freedom of information request, Appendix B, (No 1414950/22 dated 9<sup>th</sup> December 2022), reports that... "staff within the digital forensic unit are trained in grading indecent images of children and hold formally recognised accreditation similar to staff from the NCA. "All trainers attend the Grading of Child Sexual Abuse Material course held by the College of Policing... "They then deliver a course called Grading of Child Sexual Abuse Material to staff, which makes them nationally accredited".

Finally, the last freedom of information request, Appendix C, (No 1544A/22 dated 14<sup>th</sup> November 2022) reports that "All online child sexual exploitation team staff undertake detective training and the specialist child abuse investigators development programme (SCAIDP)...Some officers have completed training by the National Crime Agency, which has recognised them as Nationally Accredited Image Graders".

When exploring the FOI requests, several differences are noted between each police force. If we first look at image grading training, differences are noted between each police force and the participants within this study. Notably, it appears that staff within the first FOI request who hold Home Office-approved image grading training are accredited and qualified to train other officers. However, the officers who receive the secondary training are not accredited in this skill area.

In a similar vein, the second FOI request reports that staff within the digital forensic unit in this particular police force also hold Home Office-approved accredited training in image grading which then allows them to train other members of staff who then become, 'nationally accredited'. However, It should be noted that digital forensic units within the police service are those who typically examine and interrogate devices seized from suspects for all types of offences and are not front-line investigators.

Whilst the differences within image grading training are noted, the final FOI request, Appendix C, claims that all officers and staff in their online child sexual crimes exploitation teams have completed the Specialist Child Abuse Investigators Development Programme course, (SCAIDP). In addition, some of their staff have also completed the NCA's nationally accredited image graders course. As a result, it could be suggested that the officers and staff within this particular police force are trained in the investigation of both online and physical child sexual offences. Subsequently, there is a reasonable argument to suggest a standardised approach to online CSEM offending investigation where officers and staff have similar training. Suffice it to say, that from the FOI requests at least, there appear to be inconsistencies in how some police forces train their staff in image grading and the overall training and qualifications required as standard for CSEM investigations.

Regarding the SCAIDP training as mentioned in the FOI request, this course is a standard safeguarding course used by police and Social Services which primarily addresses physical sexual offending but also involves some input regarding online CSEM offences. When discussing the usefulness of the SCAIDP course for participants in this study, it was interesting to hear the narrative of one participant who felt that this course was unnecessary for their role.

Dan, DC, online sexual crimes unit: I think the SCAIDP (course) is preferable, but again I doubt the SCAIDP portfolio really fits what we do; we are a very niche world.

(Parenthesis inserted by the researcher)

The interviewee's views on the SCAIDP course may relate to its primary role in tackling physical contact sex offending rather than online sex offences, however, the SCAIDP course has some input regarding online sex crime offences, including sexual grooming. Resultantly, these FOI requests highlight differences in the accredited training of staff working in online sex crime investigations related to their image grading and work practice. Subsequently, detective status and image grading training appear to be the standard lenses through which staff in this study working on online sex crimes are viewed.

Thus far, this study has highlighted some differences regarding online sexual crime investigation training and qualifications. The training surrounding the grading of indecent images appeared to be a requisite of working within the online sexual crime unit. Moreover, image grading training was essential to the participants' roles. The grading of indecent images is discussed within Chapter 2, the literature review. However, it is beneficial to remind the reader of what this entails. Indecent images of children are classified from A to C, with A being the most serious, usually involving penetration. Category C involves naked posing, while category C depicts what is often termed' naturist images.

#### 4.5. What are the difficulties in image grading training?

The grading of indecent images was standard training for all interviewees working within the online sexual crimes unit and involved traditional classroom-based training methods. This method is standard practice for other police forces around the UK. From anecdotal evidence, image training for investigators usually lasts a day or six hours within a classroom-based environment. Difficulties within image grading were noted where image grading training within this study was delivered by a minority of accredited officers:

Claire, DC, online sexual crimes unit: I'm sure everybody will say this to you, but grading training is really hard, especially when it comes to category C.

Dan, DC, online sexual crimes unit: But grading is subjective. As a grader, I am quite cautious.

Most interviewees in the study shared their experiences of grading images after completing their training—significant problems related to category C images, which were often difficult to judge. In addition, grading images was seen as subjective, relating to category C images. Glasgow (2010) addresses the problems of grading category C images by claiming that while highly explicit sexual images of children are easy to identify, it is more challenging to delaminate less explicit images, which include category C. Under the circumstances, the discussion on category C image grading deserves attention.

Interviewees within this study suggest that category C images are often treated with more caution due to their subjectiveness. For example, Kloess et al. (2019) argue that under current legal guidelines, determining if an image is posed or erotic is challenging and subjective. Additionally, in the Sentencing Guidelines Council (2013), the term 'erotic posing' may mislead practitioners as there are some cases where an image is not posed or erotic. Nonetheless, the images may still be indecent if, for example, the image is a naked picture of a child who is not engaged in sexual activity, and the image focuses on the child's genital area (Kloess et al., 2019).

Another significant problem relating to grading images may relate to the sensitive nature of the images, which often plays a part in the decision-making process of the person grading the image. For instance, category A and B images are self-explanatory and straightforward, while category C images are more challenging (Kloess et al., 2017). As a result, the role of emotions may affect the decision-making process when examining lower-category images. (Loewenstein & Lerner, 2003; Franqueira et al., 2018).

The following quote by this interviewee supports the idea of sentiment and emotions affecting the decision-making process within category C images:

Alan, investigative support officer, online sexual crimes unit: You know, naturism is not a category C, so there are issues on grading because people are speaking from the heart rather than thinking, right, what am I looking at here?

When exploring emotions and the decision-making process, they have a significant and lengthy history that identifies integral emotions as a type that usually forms part of the decision-making process (Green & Haidt, 2002; Damasio, 1994). For example, Lerner et al. (2014) suggest that an individual anxious about the consequences of a high-risk decision may choose a safer option rather than a more fruitful one. Another explanation for such cautiousness suggests that grading category C images can be challenging, due to the absence of reliable circumstances, including previous known offending history (Kloess et al., 2019). Still, regardless of the difficulties in categorising category C images, interviewees all agree that category C images are no less illegal.

The claim from the interviewee of "speaking from the heart" suggests that the human element of grading category C images may be detrimental to the investigation process. One answer to this problem is for investigators to view all indecent images of children through one lens. For example, if grading category C images is subjective, is it the responsibility of investigators to make such judgements alone? This being the case, there is a need for more precise guidance on the training around category C images, which may remove doubt and uncertainty.

As Kloess et al. (2019) suggest, the lack of previous offending history should not be the yardstick for any decision-making process by investigators. Also, treating all category C images in the same manner as more severe content enables consistency within the investigation process. Yet, what is clear is that the interviewees in this study agreed that category C images should be investigated equally as other categories. Moreover, interviewees observed this phenomenon through a wider lens, suggesting that category C offences may lead to other offending behaviours:

Eddy, DC, online sexual crimes unit: And (category) C, if there is such a thing as a lesser category, but no less illegal.

Georgina: DC, divisional CID: I think A, B, or C, I think, is irrelevant when you're investigating. I think they all should be investigated the same as you never know where it's going to lead.

Alan, civilian investigator, online sexual crimes unit: The other issue I have personally is that we get bogged down with categories. Is that an indecent photograph of a child as per legislation, photographic, digital or video? But why are we getting bogged down with it, that is a sentencing tool.

Harry, DC, divisional CID: If we have intelligence that there is a category C image on there (on the device), there might be a category A or B that has not been picked up.

(Parenthesis inserted by the researcher)

So far, this thesis has noted that categories of indecent images of children should be used explicitly as a sentencing and charging tool, not as a triage method for arrest and search purposes. Kloess et al. (2019) echo this concept by arguing that it is crucial for law enforcement agencies to continually assess the reliability of the way indecent images are identified and graded. Consequently, this thesis has highlighted an underrepresented issue within the training of police officers surrounding the grading of indecent images of children. As such, further studies in this area are called to ensure that there is a level of consistency and reliability within this process.

Another factor related to image grading suggests that previous literature on this issue has often focused on the mental health and welfare of practitioners and the challenges faced by digital forensic examiners (Wilson-Kovacs, Rappert & Redfern, 2022; Franquieria, Bryce & Mutwana, 2017; Follette, Polunsy & Millbeck, 1994; Parkes, Graham-Kevan & Bryce, 2019). While the welfare of staff dealing with these sensitive issues is essential to improve the well-being of staff involved in image grading training, training should also be re-evaluated to ensure conformity and reliability.

This thesis argues that training in grading indecent images of children should focus more on defining category C images and encourage professional curiosity to look beyond what is often viewed by some practitioners as a lesser offence. Additionally, it could be suggested that all online sex crime investigators, including those within CID, should receive image grading training, enabling them to interchange roles more quickly and efficiently.

This suggestion is a viable option considering that training is classroom-based and usually takes 6 hours to complete. Using this interpretation, this thesis will argue that there is still cause for challenging the training and subjectivity surrounding the grading of indecent images of children, particularly class C offences. To finish this section, the qualifications of the officers and staff working within online sexual crimes investigation have been identified and addressed. Consequently, a natural progression from this theme involves exploring the interviewees' standards of training to carry out their roles.

# 4.6. What is the current level of training for officers investigating CSEM offending?

It is essential to gain the interviewees' narratives concerning what training they have received to work in such a profound and essential role. To address the research question, all interviewees were asked about their level of training and technical knowledge in online sex crimes investigation. Here, interviewees narrate their views on their training to enable them to work in online sex crime investigation:

Eddy, DC, online sexual crimes unit: I do not think I have had any training, actual training in this specific field of work.

Jennifer, civilian investigator, online sexual crimes unit: Honestly, I was just chucked in at the deep end, it was a two-person role, and I was doing it on my own.

Formal online sexual crime training among the interviewees appeared problematic across the board. The online sexual crimes unit participants were just as lacking in specific online sexual crime awareness and training as their colleagues within CID. Burruss et al. (2019) point out that police officers are trained primarily to deal with and investigate physical crimes, while on the other hand, Cockroft et al. (2018) argue that digital crime knowledge should not be confined only to specialist police roles but integrated across the board. Hence, the claim from Cockcroft et al. (2018) supports the thesis arguments regarding appropriate training standards for all officers and staff working in online sex crime investigations and those in CID.

The literature on the training of police officers is abundant, covering many aspects of learning theories and other topics. For example, the training relating to cybercrime investigation has produced a plethora of academic literature focusing on various learning theories, challenges, needs assessments and evidence-based policing (Koziarski & Lee, 2020; Hadlington et al., 2018; Lee et al., 2019; Cockcroft et al., 2018). Still, while exploring the levels of training within the participant cohort, it would be remiss to suggest that training within the participant's roles is non-existent. For example, a supervisor explained the training level the staff had received. As noted, other interviewees have conveyed a similar narrative by outlining what training courses they had attended. These training courses included external courses relating to the Child Abuse Image Database (CAID) and image grading.

Ben, Sgt, online sexual crimes unit: As far as staff are concerned, I think we have got through every single staff member to train them up on the systems we use. We also have CPD days that we do with the offender management unit so that we can understand from their point of view.

Ian, DC, online sexual crimes unit: I have been lucky enough to go on some external courses while I have been here, with the NCA, things like CAID. (child abuse image database)

(Parenthesis inserted by the researcher)

Despite the interviewees highlighting their levels of training, it was apparent that the training they had received did not always relate to online digital knowledge or social media awareness. In addition, one interviewee claimed that staff had attended continuing personal development training (CPD) and seminars on criminology and victimology. Despite this, no mention was made of training regarding digital technology or social media awareness used in online sexual offending. The interviewee also mentions that staff have been trained using "their systems;" however, it is unsure what these systems are.

Another interviewee uses an interesting phrase, "lucky enough to go on some external courses". Using the term. "lucky enough," the interviewee may suggest that training courses are infrequent and not the norm. In contrast, one interviewee implies that finding suitable training courses is their responsibility rather than the organisation's. It should be noted that this interviewee claims that any training requests are never refused. Nevertheless, this interviewee is a civilian engaged in victim identification and safeguarding, not in the front-line investigation role. Resultantly, the courses attended by this participant are not offered to other participants:

Jennifer, civilian investigator, online sexual crimes unit: To be fair, there is no set training.

It is just a case of me finding out what I can go on; they never refuse me training.

Eddy, DC, online sexual crime unit: So, extra training would be helpful. I did not get any and had to learn from colleagues.

Harry, DC, divisional CID: Because, a lot of time, we just learn as we go along.

Discussing the interviews, the participants narrated their training regarding online sex crime investigations. The omission of social media awareness training and knowledge of digital platforms used in online offending is noted. Moreover, Cockcroft et al. (2018) argue that criminal justice agencies have been slow to engage with and adapt to new interactions between criminal behaviour and technology. On the contrary, Marcum et al. (2010) point out that high-quality, specialised training relating to the possession of child abuse material does not improve the quality of successful investigations but rather the use of appropriately skilled personnel.

While McCrum (2010) may be correct in suggesting that appropriately skilled staff are essential to effective police investigations, one cannot ignore the benefits of highly trained officers with a specialised knowledge of social media and online digital platforms used in online sexual offending. Also, online offending technology and social media platforms have vastly evolved over the past decade, making online CSEM offending easier. That being so, this technological evolution calls for a more robust policing approach to training related to tackling online sex offending against children.

After addressing both sides of these arguments, this thesis has highlighted a lack of appropriate training in online sexual crime investigation when dealing with crimes facilitated by social media and other online digital platforms. As online technology and social media have evolved dramatically in recent years, police officers working in online sexual crime investigations should be better prepared to meet this challenge. In these circumstances, training should reflect the importance of social media and other digital platforms in online offending.

### 4.7. Additional training needs for staff

This thesis so far has highlighted the training and qualifications officers and staff in this study receive when investigating CSEM offences. The following section explores additional and suitable training options for the participants. Participants were open about their lack of formal training per se regarding online sexual crimes investigation:

Harry, DC, divisional CID: I would like to improve my knowledge in this field because it's something that's never going to go away.

Frank, DC, online sexual crimes unit: I also think we need specific training, and I have said this for a long time about the applications from which are referrals are coming from.

It is well documented that online child sexual offending has been a constant source of police investigations for decades. Interviewees refer to the prolonged consistency of online sex crime offending and the need to understand the social media applications used by the offenders. Most participants did not indicate what specialised training they would like to receive to improve their working practice. Nonetheless, the participants' lack of creative training ideas could result from their current knowledge of digital platforms and other online technologies.

Specialised police training significantly reduces offending rates within sexual offences Tidmarsh et al. (2020) and Stern (2010). Moreover, Darwinkle, Powell & Tidhmarsh (2013) detail the effectiveness of specialist police training in improving performance and investigative outcomes in sexual crimes investigation. Despite this, a fundamental problem surrounding this research relates to specialised training within physical sex crimes investigation, such as rape, rather than online sexual offence investigation. Consequently, the literature regarding the differences between physical and online sexual crime investigation is noted.

As mentioned previously in this chapter, being an investigator does not necessarily mean that all crimes are investigated similarly. For example, online sexual crime training requires a different approach to physical crimes. Cyber-dependant offences such as online child abuse rely on the IT systems necessary to commission a crime (Wullen & Kranenbarg, 2019). Accordingly, officers working in online sexual crimes investigation should be confident in their knowledge and trained appropriately.

Despite the interviewees being unsure what further training they would prefer; this thesis argues that the onus should lie with the employer regarding allocating appropriate training and resources. Accordingly, Owoyemi et al. (2011) suggest that organisational leadership should acknowledge and accept that staff training can embellish organisational performance, leading to better employee commitment and staff retention.

Consequently, appropriate staff training should be identified by senior leadership as a matter of course, yet, identifying courses and training requirements cannot be achieved unless senior leadership and management identify a need.

Identifying appropriate training courses can only be achieved by communication with front-line workers. Moreover, Kalogiannidis (2020) claims that effective communication within a business model is vital in enhancing performance as it influences planning between staff and the employer. Although Kalogiannidis (2020) refers to business organisations, it is reasonable to suggest that the theory can also be implemented within a policing environment. In that event, asking what training courses would suit the interviewees' needs is appropriate given these discussions.

Interviewer: Do you feel your training is satisfactory and if not, what could you suggest to improve your knowledge?

Kelly, DC, divisional CID: I would like training on new things which are coming out, like new apps, and I would love training to be able to get your head around a mobile phone report.

Dan, DC, online sexual crimes unit: I would like to have more conferences and CPD around the country. Because from what I have seen, we are a very close-knit bunch, and we have got lots of ideas.

The interviewees give differing opinions on suitable training ideas for increasing their knowledge of online applications used in offending. Training related to conferences and CPD as a method of improving knowledge was noted. Despite the different training approaches offered by the interviewees, it is apparent that specialised training in online sexual crimes investigation is appropriate. Appropriately, Eggins et al. (2021) suggest that specialist training within online child sexual exploitation investigation positively impacts police officers' knowledge and legislation.

Previous studies have stressed the importance of exploring police officers' perceptions of sexual crime investigation to enhance their skills and future training needs (Wright & Powell, 2007) in Tidmarsh, Sharman & Hamilton (2021). Yet, despite participants embracing the idea of further enhanced training, an interviewee claimed this was unnecessary to enable them to do their jobs effectively.

Georgina, DC, divisional CID: Sometimes, specific training is not needed to be able to do it effectively (online sex crimes investigation), but it would definitely help.

(Parenthesis inserted by the researcher)

One explanation for the interviewee making this claim could be related to their comparatively younger age than other interviewees and degree education. Upon exploring this concept, it would be remiss to claim that age alone contributes to high-level internet and online digital skills. For example, it has been claimed that higher education levels and income significantly enhance internet skills in both younger and older adults (Hargittai, Piper & Morris, 2019; Correa, 2016). So, despite factors including age and education, the interviewee may have an advantage over other participants regarding their knowledge of online offending technology compared to other colleagues.

To support this claim, the same interviewee was more knowledgeable than other participants when discussing Tor networks, online technology and the primary social media platforms used in online offending. This knowledge was not learned through formal training but rather from informal self-learning. When describing informal learning, Pereira, Fillol & Moura (2019) claim that informal education or 'internet self-discovery' is motivated by an individual's needs and colleagues' influences. Nevertheless, senior leadership must address this by communicating with their staff regarding their training needs. Consequently, specific online technology training for officers and staff should be the responsibility of the organisational leadership.

It should be noted that officers and staff also have a degree of personal responsibility regarding their continuing professional development and should avail of personal learning and responsibility. Addressing this, Stockdale and Brockett (2011) argue that self-direction is recognised as an essential factor in the adult learning environment. Moreover, Glass (2013) claims that an education system should endeavour to seek out and enrich personal responsibility in learners. Accordingly, this thesis addresses the issue of further training needs by highlighting the responsibilities of senior leadership and the personal responsibility of staff to keep themselves updated through self-directed learning and CPD.

Despite personal responsibilities in identifying training needs, a minority of interviewees were specific in what training they wanted, which included more information on technical reports and social media applications. Also, attending more conferences was mentioned by one interviewee. Thus, It would be beneficial for future research to address these issues by exploring the training needs and wants of officers working in online sexual crime investigations. In this vein, this thesis argues that policing leadership address the need for appropriate role-related training and CPD for their staff including regular updates on online technology, the most popular social media platforms used for grooming and in-depth knowledge of peer-to-peer networks and file-sharing sites.

The following sub-section explores how a lack of training in online digital knowledge and social media awareness can affect police investigations and confidence. For example, interviewees voice concerns regarding suspects possessing more knowledge related to social media used in online sexual offending and a lack of confidence in their knowledge of social media applications.

## 4.8. The training and awareness of online digital platforms and social media

When exploring the literature, there are minimal academic contributions regarding police officers' knowledge and training of social media and digital platforms, (Evensted 2017; Dodge & Burrus, 2019; & Cummins, Florey, 2016). Viewed in this way, it is essential to address this issue by acquiring the participant's perceptions of social media knowledge, awareness and training:

Georgina, DC, divisional CID: Some people have a good knowledge base, and people have none at all; some people are absolute technophobes through no fault of their own; however, it's just the way they are.

Aside from day-to-day police investigation, this study's participants' working environment involves online digital technology and social media knowledge and awareness. The study participants have much experience working in online sex crime investigation, even so, the question should be asked: can officers effectively investigate online crimes involving new technology and social media without sufficient prior training and knowledge? Considering the interviewees are front-line police investigators in online sexual crimes investigation, their knowledge of social media and digital platforms appeared inconsistent given the serious nature of their role. Here, the interviewees highlight the limitations of their colleague's social media and digital knowledge and awareness:

Ian: DC, online sexual crimes unit: Now there are people in here who, to term it nicely, are Luddites and have no kind of computer knowledge or anything, which is fine because we have people in here who are very, very good.

Frank, DC, online sexual crimes unit: What you tend to find is that the techier people are better at understanding.

When examining the responses from the interviewees, ordinarily, comments such as 'Luddites' would appear out of place in a specialised front-line policing unit tackling online sex crimes against children. Notably, one interviewee claims that 'techier' colleagues are more informed regarding online technology, suggesting that a lack of online digital knowledge within their working practice was to be taken for granted. In addition, the term 'Luddites' used by one interviewee is interesting.

This term is also discussed by Milivojevic (2021, p.3) when they suggest that "there is a growing network of modern Luddites" who "call for restraint and, often, a dramatic rejection of new technologies."

When using the term Luddite, Milivojevic (2021) appears to be addressing the perceived outcomes of digital technology and the reluctance of individuals to embrace it. Yet, this concept is not new, especially within the policing environment and dates back many years. For example, in the article on the impact of technology on police management, How (1980, p.338) writes, "The grail of technology is typically introduced into an organisational milieu characterised by conservatism and ignorance". Today, How's (1980) comments may appear outdated, given the vast improvement and deployment of policing technology; however, when discussing the issues of social media knowledge and online technology, some interviewees still appear to lack appropriate knowledge and training on this subject. Thus, this prompts the question, are some individuals unwilling to embrace online technology despite this being related to their profession?

A possible answer to this problem by Costinot & Werning (2018) suggests that as technology becomes efficient, society will become more "Luddite". Despite this claim, is this a fair assumption, given that some individuals have grown up with technology and could be perceived as having an advantage over those who acquired digital technology later in life? This theory was previously discussed by Jewkes & Andrews (2006), who suggest that technophobia amongst police may gradually disappear as more individuals who have grown up with digital technology join the police. For that reason, it could be suggested that younger individuals who have grown up alongside online digital technology should be more favourable to embedding technology into the learning environment (Autrey & Berge, 2011).

Yet, over 15 years from Jewkes & Andrews's (2006) claim, are police officers who have recently entered the police service any better informed on online technology than their colleagues who joined many years previously? In this case, this question calls for further investigation using qualitative analysis and age demographics of officers working in online sex crime investigations.

Moreover, It should be noted that participants in this study's age demographic ranged from their late 20s and mid-30s to their late 40s and early 50s. Keeping this in mind, the age differences in the participants in this study suggest that some have grown up with the internet and social media, while others have adapted to it later in life.

Having said that, just because an individual has grown up with online technology does not necessarily mean they are more proficient than those who adapted to it later in life. Wang et al. (2019) highlight this issue when they claim that those who grew up with online technology have a stronger preference for IT use, although the extent of using such technology and their digital skills are not always compatible with other younger individuals. Illustrating this, some individuals who adapt to online technology later in life exhibit abundant diversity relating to their online skills and specialised experience (Choi & Di-Nitto, 2013; Gell et al., 2013; Mitzner et al., 2010). Despite these issues, there should be crucial mechanisms to address this problem within the policing environment, which include education and specialised training in cybercrime (Hadlington et al., 2018).

The use of the word 'technophobe' by one interviewee is interesting, given the operational role of the participants. When exploring the concept of technophobia, evidence by Khan (2015) suggests several reasons why technophobia among the police an issue is. For instance, as Khan (2015) alludes, these issues relate to an aversion to learning new skills, the fear that technology will erode traditional policing skills, and enhanced organisational and public accountability. As a deduction, when further examining technophobia within policing, the literature tends to focus on police technology, including 'hard tech' such as body-worn videos and radio communications systems, rather than the use of online platforms. (Bowling & Iyer, 2019; Whatmore, Wiklef & Marten, 2020).

Technophobia amongst the police is not a new concept. Earlier work by Goodman (1997, p.479) argues that police are often slow to respond to digital crime due to "A lack of computer savvy (officers) and the fear of technology or technophobia". Notably, this earlier work by Goodman (1997) cites issues relating to technology training and use, which are still evident today.

Moreover, insufficient training in technology issues for staff and any training usually involves general law enforcement and criminal database systems. While technology has evolved rapidly since 1997, Goodman's (1997) claims are still palpable today in some aspects of policing, as social media has progressed rapidly over the last 25 years. Accordingly, evidence in this study, suggests that the knowledge and training of police officers in this genre have failed to catch up.

Similarly, Interviewees within CID highlighted their concerns when dealing with digital and social media platforms. Interviewees claimed to understand social media platforms used in online offending; nonetheless, this study will argue that some of their knowledge is limited, in line with most adults of similar ages. For example, when using social media, older individuals tend not to follow social media trends but rather stick to their favourite social media platforms (Hruska & Maresova, 2020). Unsurprisingly, mid-range adults usually favour specific social media platforms, such as Facebook, as the other popular networking sites tend to target younger age-specific audiences, which include teenagers, students, and singles (Hutto et al., 2015).

To reinforce this theory, the youngest interviewee mentions the KikApp messenger, which is still popular with a younger demographic. In contrast, another older participant cites TikTok as the most prominent social media app for online offending, yet It should be noted that this participant was more experienced in social media applications than their colleague due to their specific role when dealing with children and young people:

Kelly: DC, divisional CID: We do understand they are using different media to be able to speak to children to commit the crimes, different apps, different things like Facebook

Georgina, DC, divisional CID: I have a basic idea of what happens; by basic, I mean the platforms as in social media apps, so Kik Messenger is a big one, Instagram, Facebook, onion browsers, and Tor networks.

Harry, DC, divisional CID: I think I understand pretty much how they would do it; I would not know how to access it myself.

Jennifer, civilian investigator, online sexual crimes unit: What we found at the moment is TikTok is our biggest one, but if they have TikTok, they have Instagram as well.

A lack of confidence in social media application knowledge was not just confined to CID participants. Several interviewees cited the many social media applications as barriers to understanding how they worked. This concept was not confined to one group but across the whole cohort of participants.

Jennifer, civilian investigator, online sexual crimes unit: But every day, more are coming out (applications). It is impossible to police because another one or 10,000 will come out today or whatever.

Ian, DC, online sexual crimes unit: There are that many different platforms out there. You can't keep up with them all.

Eddy: DC, online sexual crimes unit: The internet is growing so quickly, and it is very difficult for the cops to grow and match that growth.

(Parenthesis inserted by the researcher)

As previously noted, interviewees claimed that the vast number of social media sites was a barrier to understanding how they worked or what they did. This claim could at first be understandable given that the National Centre for Missing and Exploited Children (NCMEC) receives referrals from hundreds of digital platforms annually. For example, in their 2021 report, NCMEC cites over 75,038 referrals from 300 electronic service providers, including social media platforms. Surprisingly, the minor referrals to NCMEC related to social media included Facebook and Instagram, receiving 28 and 22 referrals, respectively.

Comparing what we know about online offending and social media per se, NCMEC reports that the most extensive referrals received include Cloud-Fare, a secure network site (2,959) and Digital Ocean, a cloud hosting provider (2,685). Accordingly, the data contradict what is known about the leading social media platforms used for online sexual offending, as Chapter 2 of the literature review suggests, Facebook and Instagram are the leading social media platforms used to groom and sexually exploit children (The Internet Investigation Report, 2020).

Regarding the participants' claims concerning the vast number of social media sites being a barrier to knowledge, a basic Google search will offer hundreds of sites highlighting the leading social media apps considered a risk to children. Moreover, most sites list and explain how these social media apps work and other helpful information. For example, Table 4.1. Kemp (2022) illustrates the most popular social media apps globally in 2022, with WhatsApp as the leading application. Again, the data contrasts with what we currently understand about current social media use.

Table 4.1. Kemp (2022) Leading Social Media Apps Globally in 2022, Data Reportal

Social Media App	Global Percentage Use
WhatsApp	15.7%
Instagram	14.8%
Facebook	14.5%
WeeChat	11.4%
TikTok	4.3%
Twitter	3.3%
Facebook	2.6%
Telegram	2.0%
Line	1.8%
Pinterest	1.8%
QQ	1.6%
Snap Chat	1.4%

Despite being ranked in fifth place globally in Table 4.1 (Kemp, 2022), TikTok, is considered the UK's leading social media app for young people, with Ofcom's Media Use and Attitude Report (2022) claiming that half of 3 to 17-year-olds in the UK are now using TikTok. In response, the NSPCC (2022) highlights the online risks to children using the TikTok social media platform. For example, as TikTok uses algorithms to show users new content, it is easy for children to access inappropriate or adult content and videos inadvertently.

Moreover, TikTok also has communication features allowing users to message others privately, which may place children at risk of being contacted by a stranger (NSPCC, 2022). That being the case, from a safeguarding perspective, it is prudent for police officers and staff to acquaint themselves with the latest social media trends to see how they work, what the risks are to children and how they operate.

This thesis will claim that limited knowledge of social media apps by some front-line police officers is not a result of the large volume of online sites available but rather a lack of professional curiosity, knowledge and understanding. Upon exploring this concept further, Williams et al. (2021) report that uniformed front-line police were often confused about dealing with an offence conducted via social media besides a few specially trained officers. What is termed 'specially trained officers' is unsure; however, the participants in this study would no doubt fit these criteria.

One drawback regarding Williams et al. (2021) is that, like similar studies, the research primarily relates to uniformed front-line police officers rather than specialised detectives working in online sex crime investigations. Nevertheless, there is no escaping the influence of social media on the policing environment. As Walsh & O'Connor (2019) allude, as digital technology becomes ever-sophisticated and evolves, so will policing organisations and the public they serve. In this respect, the policing response to sexual offences facilitated by social media requires a more structured and robust attitude towards training and knowledge. Thereupon, this thesis argues that further academic enquiry into this subject is justified and valued.

## 4.9. The experience of knowledge sharing

This main section of the thesis will explore the theory of the participant's working experience and the sharing of knowledge as a learning tool. When exploring the standard of training amongst the participants, it was noted that working experience and on-the-job training were significant factors. Participants used the term 'experience' more times (*n*-18) during interviews than any other comment. In addition, interviewees also narrated how knowledge and experience gained through working practice could be passed on to colleagues. To that end, this thesis explores whether working experience increases operational effectiveness and knowledge sharing.

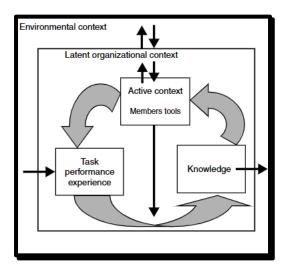
As Helyer (2015) points out, top-level skills are often associated with a higher level of education, with graduates more able to develop wide-ranging skills using their creativity and imagination. Nonetheless, It must be stated that unless declared, the participants' secondary or university education levels were unknown during the interviews, aside from two CID detectives with university degrees. When examining the concept of education within the workplace, Heyler (2015) claims that graduates or those with higher-level qualifications are more sought after by employees due to their analytical skills, critical debate, and creativity. In contrast, Boud, Cohen & Walker (1993) claim that formal education has prompted minimal knowledge, with individuals learning more from other sources of influence.

To strengthen this argument, Boud & Walker (1991) would argue that regardless of how much training and formal education individuals receive, they are not equipped for responsible roles unless they can learn from experience. Addressing this theory, Argote & Miriam-Specter (2011) claim that at the centre of most organisational learning is a change that comes about as the organisation gains experience. For example, the participants in this study appear to have a vast amount of experience in their role. Nevertheless, it is crucial to understand how this experience is gained, retained, and shared. Consequently, it could be argued that participants in this study have gained knowledge and experience by working in the same role for over five years or longer.

Despite the participants having held long service within their operational role, the experience may not necessarily lead to learning (Yip & Wilson, 2010). In addition, Yip & Wilson (2010) argue that learning from experience involves a reflective process that can be improved by adopting appropriate systems and development. Accordingly, enabling effective learning through experience requires a structured theoretical framework that enables organisations and individuals to change and adapt to transfer experience into knowledge effectively.

One theoretical framework discussed by Argote & Miriam-Spektor (2010) aims to break down organisational learning to make it efficiently managed and more relevant through various cycles. Exploring Fig 4.1. Argote & Miriam-Spektor (2010), this theory demonstrate an ongoing cycle where performance and experience are converted into knowledge, thus altering the organisation's overall framework, and affecting future experience.

Figure 4.1. Argote & Miriam-Spektor (2010) Theoretical Framework for Analysing Organisational Learning



The latent organisational context of this study relates to the everyday workings of the online sexual crime unit. For example, the unit within this study is not typical of everyday policing units, and their knowledge and experience are very niche compared to other policing departments. Moreover, previous work by Ingram & Baum (1997) and Haunschild & Sullivan (2002) claim that specialised units, such as online sexual crime units, have been shown to learn more from experience than commonplace or general organisations. Despite this, counterarguments suggest that learning from experience can inhibit the organisation by allowing staff to fall into a routine where skills are perfected yet become progressively outdated (March 1991; Levinthal & March 1993; Simon, 1993).

In the case of this study, participants continue to perform the same investigatory role using the same format and strategies, they will follow the same trajectory of arresting and interviewing suspects without intervention. This pathway is a natural progression within the police service, as their primary function is to arrest individuals suspected of committing crimes, thereby maintaining law and order. Nevertheless, modern policing needs to move beyond this concept as society becomes more reliant on technology and workers acquire new skills.

Sungsup et al. (2019) posit that in a society of modern technology, workers' skill demands require the ability to strengthen their learnability and the willingness to learn, unlearn and relearn. Using this interpretation, learning from experience within specialised units should be a process where leaders can formally use knowledge and experience to improve service delivery. Yet, despite this, knowledge and experience should regularly be assessed to see if they are still relevant and appropriate to meet organisational service delivery.

When further exploring Argote & Miriam-Spektor's (2010) theoretical framework, the total number of tasks within the theory quantifies the experience; for example, in the case of this study, the experience would ordinarily be measured by the number of arrests made by the participants and suspect interviews. Yet, the experience in this context should be based on more than just arrest rates. In this manner, many other measurements of experience, which in the case of this study, may involve increased digital, online, and social media knowledge and awareness (Argote & Miriam-Spektor, 2010).

Environmental contexts within the framework include outside organisational domains involving competitors, clients, and other organisations. In the context of this study, it could be argued that the offenders who use online technology to offend are competitors who wish to avoid arrest and detention, keeping one step ahead of the police. Thus, it is up to the police to be more competent and skilful than the offenders they compete with by improving their online digital knowledge and skills. Consequently, the environmental context is essential to the theoretical framework, as this can affect operational performance, arrest rates and safeguarding.

Accordingly, the active context within the theory involves the organisation's domain, its members, and the tools that interface with the organisational tasks. It could be suggested that organisational tasks in this study involve the arrest and interviews of the suspects. At the same time, the tools within this study are the technology used to detect offenders; the tools could include Internet service providers, cyber tip hotlines and the online monitoring of chat rooms (Cohen-Almagor, 2013). Then, the member-task-tool chain will designate which staff will perform the tasks and which tools will be used. Resultantly, through this process, learning occurs, and knowledge is created, maintained, and transferred.

Nevertheless, the learning and knowledge transfer within the process can only be effective if the transfer is both formal and accountable. Accordingly, leadership within organisations should ensure that staff retain and share knowledge and skills in a formal process of shared experience. Finally, organisational leadership should assess these skills, knowledge, and experience regularly to ensure they do not become outdated or irrelevant.

The differences between experience and qualifications were mentioned during participant interviews. The issue of experience, as opposed to qualifications, is not a new concept within the police service. Highlighting this, Hoggett et al. (2019) explore the controversial subject of direct entry police inspectors and superintendents appointed without requiring entrants to work their way up the ranks. Taking this into account, Hoggett et al. (2019) reported that most participants would agree that previous experience as a police officer was needed to be an efficient police leader. Here, the following quotes from the Interviewees highlight their views on working experience, which were essential aspects of their operational role. Moreover, the experience was considered more valuable than qualifications, training, or courses:

Claire, DC, online sexual crimes unit: We are a really experienced unit, and nothing goes out to anyone what isn't wanting to deal with that type of work.

Ben, online sexual crimes unit: Like a lot of things in the police, it's the experience of working that gives you more learning than the actual courses themselves.

Frank, DC online sexual crimes unit: I think there is a lot to be said for training and education within units; we tend to educate ourselves through experience and the experience of others.

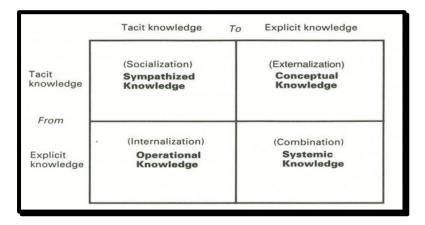
It could be implied that the Interviewees suggest that working experience outweighs formal training and education, though, this claim is reasonable, given some of the interviewees' length of service and role. On the other hand, Laurillard (1993) argues that there are differences between learning in the natural world and learning within the organized world of higher education. For example, learning from everyday experience happens by chance, and how we learn depends on the current situation (Laurillard, 1993). As a result, any knowledge captured or gleaned must be used to its full potential.

Despite this idea, the quote from one interviewee, "We tend to educate ourselves through experience and the experience of others", would suggest that an individual can pass on their knowledge to others once they have specialised knowledge of the content or subject matter (Gauld & Millar, 2004). To this end, as Gauld & Millar (2004) agree, specialist knowledge of a subject was not necessarily a requirement of efficiency within the role.

One critique of Gauld & Millar (2004) would argue that experience within the role of online sexual crimes investigation requires some degree of specialist knowledge relating to the suspect demographic and the sensitive nature of child abuse investigations. For example, online sexual crimes differ significantly from other crimes in how they are investigated and reported. To this end, there is a strong argument for the participant's claim to learn from each other's experiences and educate themselves by sharing knowledge. On the other hand, this chain of learning and sharing knowledge should be carried out systematically and accountable.

According to Nonaka & Takeuchi's (1995) SCEI model (1995), Fig 4.2., knowledge is a process that is initially socialised by becoming tacit, externalised, combined, and then internalised. Moreover, the SCEI model is a continuous process, is simple to use, and explains the knowledge conversion process (Zhaung & Tongxin, 2010). Furthermore, Adesina & Ocholla (2019) claim that the SCEI Model can be used effectively within organisations for knowledge-creation activities, enabling knowledge sharing. Suitably, this model of implied knowledge can be used successfully by police leadership within a policing environment.

Figure 4.2. The SCEI Model (Nonaka & Takeuchi, 1995)



The socialisation mode of this model implies that leadership within organisations must monitor the model closely for effective knowledge management (Adesina & Ocholla, 2019). As a result, leadership should be more in tune with active learning and acquiring and sharing knowledge. Despite the claim, this can only be achieved if leadership within organisations understand the nature of learning theories and can transfer these skills into the work environment. Thus, leadership and management must be responsible for learning and knowledge sharing to be effective within the workplace and organisation.

As with most theories and models of learning and knowledge, some caution must be taken. Adesina & Ocholla (2019) noted some weaknesses within the SCEI model in their comprehensive review. For example, the model sees the transfer of knowledge as a sequential process when this may not reflect real-life situations. Also, Tuomi (1999) suggests that the structure of the Nonaka-Takeuchi (1995) model is too egocentric, making it challenging to depict interactions and abilities across various layers of scrutiny. Despite the limitations of the Nonaka-Takeuchi (1995) model, this thesis argues that shared knowledge, experience, and learning within the policing organisation should be both formal and accountable.

To summarise, Informal learning was accepted as a way of sharing knowledge without sending all officers on seminars and courses, saving time and money. Howbeit, this thesis will ask if this is an exemplary process of sharing valuable knowledge in an environment such as an online sex crime investigation. Also, the danger of misinterpreting second-hand knowledge, which has been shared informally, is a factor of note. For example, when exploring the concept of previously known knowledge, Hug & McNeill (2008) define first-hand knowledge as occurring when individuals investigate a phenomenon with a hands-on approach to inquiry. On the other hand, second-hand learning involves understanding and evaluating other individuals' investigations and knowledge (Magnusson et al., 2004).

Understanding how other individuals can capture, share, and retain knowledge is vital if organisations are to achieve their full potential. Nonetheless, despite how knowledge is gained, individuals and organisations may be challenged to validate the relevance and trustworthiness of the information gained (Feucht, 2017). Finally, passing on knowledge to others within an organisational context should be formal and structured using an appropriate theory or model. Using robust measures will ensure that the learning and sharing of knowledge processes are accountable and reliable. Under the circumstances, future investigations within this concept should explore the appropriate and accountable methods of sharing knowledge and learning.

# 4.10. What is the impact of police officers' knowledge and changes to online offending behaviours?

Although the primary focus of the research question relates to the participants' training and knowledge of online sex crime offending and technology, identifying the changing nature of online offending is an essential aspect of the research. Using this knowledge correctly is essential regarding future training and research, helping to develop technological countermeasures and bespoke training packages. This being so, this thesis will argue that this knowledge is not being used to its full potential.

Chapter 2 of the literature review notes that online sex offenders are not a homogenous group but rather heterogeneous, displaying different facets of offending behaviours (Babchishin et al., 2018). In addition, the previous literature has focused on the differences between online and physical contact offenders and sexual addiction (Brown & Bricknell, 2018; Henshaw, Ogloff & Clough, 2016; Elliot et al., 2009).

Also, as discussed in Chapter 2, Broadhurst (2019) points out that child sex-offending behaviour differs as some offenders engage in physical contact while some produce and distribute indecent images of children. In addition, others view indecent images, while other online offenders may become contact sex offenders. Because of this, it is vital to note any changes and differences in offending behaviour by those who deal with it daily.

Noticing changes in online child sexual offending behaviour is difficult as qualitative academic studies with the offenders are challenging. Difficulties within the recruitment process of sex offenders are often due to mistrust, developing rapport and the experiences of guilt and emotional vulnerability amongst the participants. (Klein et al., 2018; Dickson-Swift et al., 2007). Finally, the next best option for capturing data on noting changes to online offending behaviour is a qualitative exploration of those dealing with offenders and their offending behaviour. Ergo, for this reason, this thesis addresses this critical issue through a qualitative study with front-line officers working in online sex crime investigations.

Moving on, interviewees narrated their observations regarding the changes they had witnessed in suspects' online offending behaviours. The phenomenon of sexualised chat offenders and sexualised groomers accessing and sharing indecent images of children appears to be relatively unexplored. Moreover, most of the past and current literature relates to the risk of physical cross-over or progressive offending behaviour related to sexualised chat or grooming (Babchishin et al., 2018; Webb, Craissati & Keen, 2007; Babchishin, Hanson & VanZuylen, 2014). The typologies of online sex offenders are explored in Chapter 2; however, this thesis will argue that in this study, online sex child sex offenders are now offending across all levels of sexual deviancy including sexualised grooming, physical contact offending, possession of indecent images and sexualised chat with children.

Recent evidence suggests that indecent image offenders are a heterogeneous group with smaller sub-groups of typologies related to behaviour and sexual interest, including sharing and accessing indecent images and other sexual interests. (Gottfried et al., 2020). To further expand on Gottfried et al. (2020), according to the interviewees, there are more facets to online offending behaviour than what is currently known. More notably, the interviewees discuss the significant changes in online offending behaviour related to online sexualised chats with children and possessing and sharing indecent image offences:

Dan, DC, online sexual crimes unit: What you will see as well, some of the chatters will distribute indecent images as a way of making themselves seem more viable as a child abuser.

Eddy, DC, online sexual crimes unit: You tend to find that they are committing other offences once you have had their equipment analysed, so if they are having a sexual chat with children, oftentimes they possess images.

Frank: DC, online sexual crimes unit: It is seldom that we will find somebody who is chatting online with children or adults who will not, as part of that conversation, come into contact with child abuse imagery.

The rise in online sexualised chat offending against children is a concern and is often underreported in current academic literature. Earlier work by Seto et al. (2012) highlights the limited evidence on the behaviours of the chat room and online solicitation offenders. Similar findings have also been reported by De-Hart et al. (2016). Nevertheless, contrary to what has been previously accepted, the interviewees highlight the concerns of online offenders sharing indecent images while engaging in sexualised chat with children or other like-minded individuals.

The interviewees noted that while there are changes in online offending behaviour, there appears to be no official method of using sharing or storing this information. Whilst this knowledge may be anecdotal amongst the interviewees and their colleagues, the data is vital and should be captured to reinforce academic investigation in this area. Participants also mention the significant rise in sexualised chat offences, which have grown over the previous five years. Also, one interviewee narrates how sexualised chat offences are now on par with indecent image offences:

Eddy, DC, online sexual crimes unit: Five years ago, you might get a chat job every six to eight weeks; now, it is three or four a week.

Claire, DC, online sexual crimes unit: It used to be that the majority of our work was indecent images, but now I would say that it is at least fifty / fifty (sexualised chat), in fact, maybe slightly, probably more (because) of the UCO (undercover officer) work.

(Parenthesis inserted by the researcher)

One explanation for the recent growth in sexualised chat and grooming offences over the previous five years could be related to one participant's comment regarding undercover officers (UCOs) who deploy on known chat sites posing as children. The use of undercover police officers on chat room sites is well documented in Kloess et al. (2017) and Davis (2020). Moreover, the history of undercover police officers deploying on internet chat forums was first conceived in 2004; however, this was only to monitor the chat sites instead of officers going undercover as a child (The Guardian, 2004). In 2017, online undercover officers (UCOLs) were deployed nationally to tackle this increasing phenomenon (College of Policing, 2021). Resultantly, this time frame, 2017-2021, appears to fit in with the suggestion from the interviewee regarding the rise in chat offences over the previous five years.

The time frame may also explain the increase in sexualised chat and grooming referrals compared to indecent image offences. Nevertheless, there should be a note of caution regarding this claim. For example, there may well be other reasons why the rise in sexualised chat offences has increased, including changes in online technology, improvements in online device technology and the Covid-19 pandemic. Thereupon, this theory is worthy of further exploration and study and will be discussed in Chapter 5.

Quantifying and cataloguing changes in online offending behaviour are essential factors in how organisations can deliver practical and effective training. Failing to account for the number of specific offences can lead to discrepancies within organisational effectiveness. For this purpose, this thesis argues that while officers note changes in online offending behaviours, organisations and police leadership fail to use or catalogue this knowledge correctly. Here, interviewees provided conflicting evidence from other colleagues regarding offending sexualised chat behaviour:

Ian, DC, online sexual crimes unit: I would say that we probably get more, and this is not meant to sound belittling, more standard image jobs than chat jobs, I would probably say, seventy/thirty, or sixty/forty.

Eddy, DC, online sexual crimes unit: I would say I have got a good seventy per cent, I would say, of the jobs that start off as a chat-type jobs develop into an image jobs as well.

When exploring the quotes from the interviewees, It is interesting to note some discrepancies within the volume of sexualised chat offences compared to image offending. Suitably, this thesis argues for adequate methods of monitoring and quantifying offending behaviours, enabling organisations to focus on bespoke training, knowledge sharing, and intelligence gathering.

The interviewees also noted other changes in offending behaviour. Due to the participants' experience interviewing suspects, they can observe changes in online offending behaviour that would otherwise go unnoticed. Moreover, another facet of the qualitative interviews explored the concept of online image offenders who also engaged in contact sex offending with children. While previous literature has discussed this phenomenon, it was essential to understand the participants' experiences:

Dan, DC, online sexual crimes unit: The images are not doing it for them anymore, or they have never been image offenders; they just want to abuse or want to engage in that chat around child abuse.

Eddy, DC, online sexual crimes unit: I have got an investigation which I will not go into details about; it came from an online chat investigation about computers being analysed, but I identified a contact victim from thirty years ago.

Kelly, DC, Divisional CID: A lot of it would be adult males sending pictures of their penis, or then it will be grooming offences such as inciting a child to engage in sexual activity and then trying to meet up with them.

Interviewees claim that in their working experience, online offenders who engage in various types of offending will, at some point, want to meet up with a child for physical or contact sexual abuse. Interviewees base these claims on their experiences interviewing online child sexual exploitation suspects. Yet, the interviewees' claims contradict the current literature on the subject. The literature on online cross-over or progression offending is extensive and often relates to offenders' risk factors and predictive behaviour (Gott-fried et al., 2020; Babchishin et al., 2018; Magaletta et al., 2014).

The literature on this subject is also divided regarding the risk of cross-over offending. For example, Magaletta et al. (2014) argue that online-only sex offenders who target children do not directly engage in physical contact but employ secondary noncontact offending. Under the circumstances, secondary noncontact offending could include live streaming and peer-to-peer chats with like-minded individuals. Further contradictory evidence from Babchishin et al. (2018) claims that online child sexual exploitation is not always an entry to physical contact and sexual offending against children.

Houtepen et al. (2014) report that most online image offenders do not engage in physical contact offending. Proportionately, others would argue that the risk of grooming or chat offenders engaging in physical contact offences with children is minimal (Gooschalk, 2011; Briggs et al., 2011; Whittle et al., 2014).

As noted, discrepancies within academic literature are evident regarding the risk of contact or cross-over offending are apparent. Regardless, it is only by listening to the experiences of interviewees and their working experiences that a different offending picture emerges.

According to the interviewees, it is evident that online sex offenders are engaging in the whole spectrum of child sexual offending, including possession of indecent images, grooming, sexualised chat, image offending and contact sexual abuse.

# 4.11. The use of social media knowledge and awareness during suspect interviews

When further discussing the interviewees' online digital knowledge and social media awareness, some concerns were raised regarding their online knowledge and training compared to the offenders. Capturing the knowledge and skills in police interview techniques is another important aspect of this thesis, which, again, addresses the lack of knowledge retention and sharing. This sub-section explores how suspect offending behaviours can be collated by officers during suspect interviews to add to knowledge and improve training and service delivery in online CSEM investigations:

Frank, DC online sexual crimes unit: But without the full knowledge of your understanding of 'Tik Tok' and how 'Tik Tok works, how potentially that upload has happened, it is very difficult to understand whether somebody is telling you the truth.

Traditionally, police Interviews of suspects are the primary methods of obtaining evidence during criminal investigations (Roberts, 2012). Previous work by Gudjonsson (2003) highlights the risks of some police interview practices, which can lead to false or inadequate information being gleaned from the suspect. This concern was raised during the interviews where a participant raised a significant issue regarding how a lack of knowledge related to social media applications might affect the course of an interview with a suspect.

The interviewees for example, reasonably assume the benefits of knowing if a suspect is lying by understanding how a social media application works before the interview. For example, earlier work by Leo (1996) argues that police officers can detect if a suspect is untruthful during an interview. In contrast, other studies suggest that police officers are no better at identifying deception than non-experts (Granhag & Stromwall, 2004; Vrij, 2000 & Memon, Vrij & Bull, 2003). Hence, it could be argued that police are more accomplished in legal areas during suspect interviews than in other issues (Clarke & Milne, 1999; Griffiths & Milne, 2005).

Although basic interview training for police has been beneficial, there has been minimal evidence regarding interviewing skills involving interviews with sex offenders. Moreover, Benneworth (2009) detail a lack of research regarding police interviews of adult-child sex offenders and how they are conducted. In this event, the issue of police interviews with online sex offenders is justified and deserves further exploration. Here, Interviewees in this study narrated their opinions on gaining knowledge from the suspects during police interviews:

Harry, DC, divisional CID: We learned quite a lot from the actual offenders that we in interview ourselves.

Claire, DC, online sexual crimes unit: We should consider intelligence interviews, especially when they are talking.

As noted, interviewees narrated the importance of gaining intelligence and information from offenders during the police interview process. Despite this, the interviewees did not routinely do this when interviewing a suspect. One reason for this may relate to police intelligence interviews being conducted with suspects related to volume crimes such as burglaries and car theft (College of Policing, 2022). In addition, one interviewee claims that they "learned quite a lot from offenders" during suspect interviews; yet knowledge gleaned from suspects is not being shared appropriately within the organisation.

In response, this thesis has already discussed the usefulness of organisations adopting learning theories and models to retain and share knowledge effectively. Equally, this thesis will suggest that training and knowledge relating to online sex crime investigation should include intelligence interviews with suspects, particularly the knowledge relating to social media and digital platforms used in offending. As interviewees suggest, gaining intelligence and knowledge is only possible if officers understand the offenders' use of online digital platforms and social media. To support this idea, it is well-documented that offenders can provide important information regarding their criminal activity and crime patterns (Decker, 2005). Resultantly, information gleaned from a suspect can be valuable to problem-solving approaches to criminal investigations.

Before one can glean intelligence and information from suspects during police interviews, officers must understand the technology and applications used in the offending behaviour. In their integrative review of technology usage trends by offenders, Steel et al. (2020) argue that although online offenders continue to use tried and tested technology to offend, many will use different techniques and methods to view online child sexual abuse content. Resultantly, the contrast in offenders' use of technology suggests a need for police officers to be better prepared to meet this challenge by being able to retain and share this knowledge. Accordingly, evidence suggests that online offending behaviour will continue to advance and increase in line with new technological advances (Quayle, 2020). In this respect, there is an organisational and societal benefit for police officers to be better trained in obtaining technology-related offending intelligence from suspects whilst in custody.

Collectively, these claims highlight concerns regarding police knowledge and awareness of social media and online digital technology overall. The lack of intelligence gathering during suspect interviews with online sex offenders is also apparent. Initially, these issues seem oblivious to the casual observer. Even so, they remain a serious concern amongst law enforcement agencies, which can only be amended by implementing social media and online digital awareness training from an organisational and personal level.

#### 4.12. Conclusion

This chapter has explored the interviews with police officers and civilian investigators who work in online sex crime investigations. Police officers consisted of detectives within CID and those working in online child sex investigations and two civilian staff working in online sex crimes investigations. Concerning the current standards of training, participants claimed that they had received no official online sexual crimes investigation training other than image grading training. However, image grading training delivered by accredited trainers allowed officers accreditation in this area once training was completed. On the other hand, evidence from other police forces through Freedom of Information requests paints a different picture. Whilst some police forces accredit officers who have received training from a Home Office-approved trainer, some forces do not.

Despite the lack of accredited or formal training, staff appeared content with their working practice and the status quo. Being an investigator or detective primarily was considered a central prerequisite for their role, despite online sexual offences requiring a different investigation approach to physical or contact sex crimes. Staff took it for granted that they could learn from each other and colleagues who were more experienced and had been in the unit for a more extended period. Notwithstanding, at the time of authoring this thesis, several of the original participants had left the unit or retired, replaced by new, less experienced staff.

The theory of experienced staff leaving organised roles is noted by Flynn & Simpson (2009) when they suggest that organisational innovation and service delivery may be compromised when staff members leave, particularly within stressful working environments. This point was noted when interviewees stressed the importance of learning from one another. Consequently, retaining and capturing knowledge formally before staff leave is essential to productive working and training.

It was taken for granted by the interviewees that official training related to online sexual crimes technology and social media was not high on the agenda by both staff and management. When exploring these issues, participants confirmed they held no official qualifications other than detective status and image grading. Despite this, the staff took this situation as routine and did not consider this much of an issue.

Formal accreditation in sexual crime investigations has been discussed in this chapter, however, none of the officers was accredited as such aside from image grading training. Illustrating this, Hughes et al. (1996, p.28), in their report of child sexual abuse practitioners, claim that there was support for national accreditation for child abuse investigators, in addition, "There should be a national standard of training to accreditation level for all those involved in child protection, from social workers, police through to solicitors, barristers and judges". While it is fair to say that today, some social workers and barristers are trained with accreditation levels when dealing with child sexual abuse, not all police officers working in this environment are.

The issue of officers working in online sexual crime accredited with the Specialist Child Abuse Investigators Development Programme Accreditation (SCAIDP) was also discussed. As previously mentioned, officers working within online sexual crime investigations do not necessarily hold this qualification. Notably, as one participant commented, "I think the SCAIDP (course) is preferable, but again, I doubt if the SCAIDP study portfolio does not really fit what we do; we are a very niche world." The comment from this interviewee may suggest that investigating online child abuse sex crimes is much different from physical contact sex offending investigations, when in fact the findings point towards offenders now offending across the whole spectrum of child sexual abuse.

Participants were also vocal about their training concerning indecent image grading. The grading of indecent images appeared to be the only prerequisite other than being a substantive detective. Several interviewees noted that grading images was primarily a sentencing and charging tool and should not be used as a yardstick of investigation priority. For example, one participant noted that "an indecent image of a child is an indecent image." Ergo, this crucial issue of note suggests that image grading training should be reevaluated to ensure a standardised approach to this problem and that police forces treat all indecent images as a singular offence rather than used as a triage for arrest importance or a sentencing tool.

Regarding working practice, interviewees spoke about the value of their working experience rather than formal training, with participants learning from each other and "learning as they went along". Learning from each other appeared essential to the participants, more so to those who were not as technically aware or digitally competent as others.

Some interesting factors were noted when exploring the interviewee's online technical and social media knowledge. For example, some interviewees had more knowledge of social media than others, using words such as 'technophobes' and 'Luddites' to describe colleagues with lesser knowledge. Duly, this disparity in online technical knowledge and skills among the participants argues for a formal approach to accredited training for police officers and staff in online CSEM investigations.

Issues of online technical and social media knowledge were raised by interviewees regarding suspect interviews. Interestingly, one interviewee pointed out how police officers may not know if a suspect is lying about using a particular social media app if the interviewing officers did not know how it worked. This again highlights the differences in the participants' levels of online digital and technical knowledge, arguing for a standardised approach to training and knowledge. Additionally, the vast array of social media apps appeared to be a barrier to knowledge for interviewees who felt that they could not keep pace with ongoing changes. To this end, improving knowledge of new and existing social media applications is possible through personal learning development and professional curiosity.

One of the interviews' most notable aspects was working experience over formal training. Compared to formal training, the interviewees stated that their working experience was essential. The Interviewees held the belief that experience rather than formal training was necessary. Interestingly, the word' experience' was used by several interviewees more times than any other word or phrase. Moreover, the relevance of the participants' working experience was noted when discussing changes in online offending behaviour. Resultantly, through their working experience investigating online sexual crimes, participants could note and observe new and emerging changes in online offending behaviours.

The changes in offending behaviours were important and included offenders now engaging in most aspects of online offending rather than specific typologies such as possession of indecent images. Illustrating this, interviewees suggested that image offenders are also engaging in sexualised chat with children, possessing and sharing indecent images and wanting to meet up with them for physical contact sex offending. Against this background, this thesis challenges what is currently known about online CSEM offending behaviour and calls for further exploration by qualitative studies with other police forces and officers working in online sex crimes investigation.

The rise in grooming and sexualised chat offences was also apparent from the interviewee's narrative. Where previously participants reported four or five incidents per month, they were now dealing with the same number per week. To explain this upsurge, one interviewee mentioned the increased use of undercover officers deployed on chat sites which may have increased the amount of arrest referrals. Despite this supposition, this theory may be consistent given the limited literature on this subject and the time frame for using undercover officers. However, this is an area which deserves specific attention from academics and policing leadership. On these grounds, this thesis argues that further work in this area should be considered by way of qualitative investigation with officers working in front-line CSEM investigation to note changes in offending behaviours.

This chapter has also identified several crucial issues related to increasing the knowledge and training of online sex crime investigators. Overall, the participants' working experience is significant in adding to our knowledge of online sex crime offending. Yet, if organisations do not understand, retain or share this experience, how can they adopt new strategies to deter and disrupt online CSEM offending? In that event, this thesis argues for a formal method of capturing knowledge from front-line investigators related to changes in online offending behaviour to improve training and research.

Responding to this concept, this thesis has outlined ways in which knowledge and experience can be used and shared by policing organisations using several theories. For instance, Kolb's (1984) learning cycle, which encompasses reflectivity in the learning process, is helpful for leadership and staff to enable effective learning and knowledge sharing. Similarly, Argote & Mirriam-Spektor's (2010) theoretical framework and Nonaka & Takeuchi's (1995) SCEI model of sharing knowledge can be used effectively to retain and share knowledge formally.

So, the apprehension and retention of experience and knowledge are essential for policing organisations and academia as learning is evaluated and used to make effective organisational changes.

To summarise, the primary findings within this chapter are noted as follows:

- Officers and staff in the online sexual crime unit in this study claimed that they had received no formal training in their role other than having detective status and image grading training,
- In this study, there was no formal mechanism or use of learning theories to capture and share any new knowledge on changes in offending behaviour that the participants had observed during their working practice,
- National accreditation for officers and staff working in online CSEM investigation
  was noted along with a standardised approach to training which included officers
  and staff being accredited alongside the SCAIPD (Specialist Child Abuse Investigators Development Programme),
- The digital and social media knowledge of officers and staff in this study was inconsistent with some of their colleagues given the serious nature of their roles with some using the terms, 'technophobe' and 'Luddite'.
- Officers and staff within this study valued experience or, 'on-the-job training' over formal qualifications.

Finally, to finish this chapter, it is crucial to understand that, as with this study, social science interviews provide helpful insight into how police officers view their ability to respond to cybercrime offences and implement new policies and working practices (Holt et al., 2018; Schreuders et al., 2020). Additionally, this thesis chapter provides an overall perspective of several important topics that impact online sexual crime investigation based on the personal accounts of police officers and civilian investigators working in online sex crime investigations.

'Cybercrime and technological advances create unique challenges to our understanding of criminality.'

(Holt & Bossler, 2015, p.17)

# Chapter 5. The Internet Watch Foundation secondary data analysis

### 5.1. Introduction

The next chapter of this thesis will explore data from the Internet Watch Foundation (IWF) from 2009 to 2022. Also, recent data from Thorn will be analysed for a comparative discussion related to the IWF data. The IWF data analysed were taken from their annual reports and related to specific topics which are relevant to the phenomenon of online CSEM offending. The overriding main headings are explored as follows: The ages of children identified by the IWF data as containing CSEM; the gender of children most identified in online CSEM; the rise in self-generated images of children; the ages of children sharing self-generated content, the changes in online technology and the risk to children and the possible causes for the increase in live-video streaming abuse.

The data from the Internet Watch Foundation will be compared with findings from the qualitative interviews to explore the possible reasons why changes in online offending and behaviour have emerged. In addition, this thesis will explore how the advances in online technology, digital platforms, and social media have changed the risk to children. Hence, the research explores how analysing the IWF data will add to existing academic knowledge and how technology industries and police organisations can improve their responses to online CSEM offending.

Again, for this chapter, online sexual harm and abuse to children will be referred to as child sexual exploitation material (CSEM). In addition, the term self-generated images of children is used throughout, although Quayle (2022) suggests that using the term 'perceived first-person child sexual abuse material' is more appropriate for child self-generated imagery. Despite this, as most of the academic and other literature refers to self-generated images, this thesis will continue to use this term.

As explained in Table 5.1., this chapter has undertaken a secondary analysis of data presented by the IWF relating to the following themes in order of hierarchy. It should be noted that exploring the data from the IWF will not include other facets which include top-level domains used; URLs worldwide; the number of complete reports; bitcoin payments, hidden services and the dark web. These omissions are due to the relevance of the initial research question, although this is not to say that these subjects are not worth future exploration.

Table 5. 1. Internet Watch Foundation-Primary Data Sets Analysed -2009-2021

**Internet Watch Foundation data sets 2009-2021** 

Changes to the ages of children identified in self-generated images,

Changes to the gender of children identified in CSEM,

The rise of the self-generated image content of children,

Changes in online technology and the risk to children,

The possible causes of online live-stream video abuse.

Before continuing with the chapter, it is beneficial to introduce the reader to the work and history of the IWF, its aims and objectives.

### 5.2. The history and purpose of the Internet Watch Foundation?

The Internet Watch Foundation was established in 1996 by several Internet service providers and the Metropolitan Police. It is a charity and a limited company that actively seeks out and removes child abuse content from the internet. Moreover, the IWF seeks to minimise the availability of online child sexual abuse content hosted anywhere in the world. The IWF also notifies all UK police forces regarding any child abuse imagery hosted in the UK or on international sites uploaded onto UK digital platforms (IWF, 2022). The IWF also provide up-to-date keywords used by online offenders and how they share them with other organisations and internet service providers. As a reminder, keywords are used by CSEM offenders to circumnavigate AI used by online service providers when openly searching for online CSEM. A fuller exploration of this use of AI is provided in Chapter 2, the literature review.

The IWF has 12 board members and publishes its policies available to the public and other organisations. Notwithstanding, as a private organisation, the IWF is not subject to freedom of information requests, unlike other organisations, including the police service. Despite the organisation's good intentions, the IWF is not averse to some criticisms. As the IWF is not an official government entity, this raises concerns from other parties. For example, most online content deemed unlawful is decided by current UK law and not a private organisation (Open Rights Group, 2020).

Controversially, the IWF has no legal authority to view child sexual abuse material, unlike all UK police forces and the National Crime Agency (NCA). Under current UK law, it is illegal to view child sexual abuse material, however, the needs of the IWF allow this to safeguard children. To combat this issue, the IWF works closely and operates with an understanding between the Association of Chief Police Officers (ACPO) and the Crown Prosecution Service (CPS), which allows the IWF immunity from prosecution. This agreement allows all IWF staff who encounter indecent images of children for legal purposes to prevent and detect online sexual offences under the Sexual Offences Act (2003) (Open Rights Group, 2022).

Yet, despite some criticisms, the IWF has removed 710,000 illegal web pages, and their analysts have assessed over 1.5 million reports of online child sexual abuse (IWF, 2022). Private donors and companies primarily fund the work of the IWF from the online technology industries, including internet service providers (ISPs), content providers, hosting providers, search providers and educational establishments. The diverse mix of online companies and organisations allows for good working partnerships and the sharing of new ideas and practices. Also, the IWF is a founder of INHOPE, the International Association of Internet Hotlines. INHOPE is an organisation that is a global network of hotlines dedicated to identifying and removing child sexual abuse material (CSEM) on the internet.

The IWF assess all reports of CSEM which contravene UK law. The process is supported by official police training, and their analysts hold the Nationally Accredited Grader certification, run by the National Crime Agency. The IWF operates under four departments: the hotline; the technical and the operations and communication with the hotline department at the forefront of identifying and removing CSEM through content analysis and image classifiers. The IWF are a vital asset to UK policing, so exploring the valuable data they have secured through their research and analysis is crucial. Finally, the IWF foundation has produced annual reports from 2009, and it is here where the data were collected and analysed.

To begin, the first main heading will commence by analysing the ages of children identified by the IWF in CSEM. This inclusion is crucial in providing a quantitative evaluation of the current state of the age groups of children who are most at risk of online CSEM.

## 5.3. The ages of children identified by the IWF in CSEM

Analysing the data from the IWF, 2009-2021, Table 5.2 and 5.3, the ages of children, who are identified in CSEM are explored. If we first explore the ages of children identified in CSEM abuse imagery, Eke & Seto (2022), claim infant CSEM was less common than prepubescent and pubescent material. Another explanation for this may suggest that infant CSEM material is much more difficult to obtain, however, as Seto (2017) notes, few offenders have this age group as a specific sexual interest.

Moreover, individuals seek out child sexual exploitation material that is sexually stimulating for them regarding age and gender (Bartov'a et al., 2021; Glasgow, 2010; Vogels & Sullivan, 2019). That being the case, Seto (2017) argues that most individuals are teleiophilic, where they are attracted to young, sexually mature adult heterosexuals. Consequently, this theory has several variations; see Table 5.4. (Seto, 2017).

When discussing sexual age preference, Seto (2017) indicates that nepiophilia remains low compared to other variations from teleiophilia. Moreover, Powell (2007) discusses nepiophilia as an individual with a sexual interest in infants and toddlers. When observing Table 5.4. Seto (2017), one can see that neophilia is rare. To support this theory, Finkelhor, Ormrod & Chaffin (2009) claim that sexual offences against children under two are extremely rare. Accordingly, the literature would agree with the IWF data, which suggests that this offending behaviour has remained static and unchanged despite the changes in online offending technology and the ease of access to relevant material.

Turning to data from the IWF, Table 5.2. and 5.3. suggests that the most prolific age group for children identified in CSEM is those aged 11-13. From 2018 until 2021 when ages 11-13 were included in the data, the age demographic remained relatively consistent, with a mean average of 59%. This age group is significant as Table 5.3. demonstrates the age group of children, 11-13 most at risk of online CSEM abuse. Another significant factor from the IWF data suggested that from 2009 onwards, there was a decrease in images of children identified in CSEM as 10 years or younger from 72% in 2009 to 23% in 2021. Thereby, it is, then prudent to ask what has caused these changes. One theory that may have caused a decline in data regarding children under 10 years of age could result from the rise in abuse images of children, aged 11-13, accounting for 7 in 10 identified instances in 2022 (IWF, 2022).

Nevertheless, according to the IWF (2022), the data relating to children aged 7-10 identified in online CSEM and self-generated images has increased by 360%. The increase in 7-10-year-old children identified in online CSEM paints a worrying picture as the increase is significant to what is already known about the high-risk group of 11-13-year-old children, particularly girls, who are the most vulnerable to online sexual abuse.

Table 5.2. Ages of children Identified in Online CSEM: 2009-2016: IWF

Year	Age (Highest)	
2009	10 or under 72%	
2010	10 or under 73%	
2011	10 or under 74%	
2012	10 or under 81%	
2013	10 or under 81%	
2014	10 or under 80%	
	11 to 15 18% 14 to 15 2%	
2015	10 or under 69%	
	11 to 15 30%	
2016	10 or under 53%	
	11 to 15 45%	
	14 to 15 3%	

\_\_\_\_\_\_

Table 5.3. Ages of children Identified in Online CSEM: 2017-2021: IWF

Year	Age Highest	
2017	10 or under 55%	
	11-15 43%	
	14-15 3%	
2018	10 or under 29%	
	11-13 56%	
	14-15 5%	
2019	10 or under 34%	
2013	11-13 48%	
	14-15 3%	
2020	10 or under 34%	
	11-13 64%	
	14-15 3%	
2021	10 or under 23%	
	11-13 68%	
	14-15 2%	

\_\_\_\_\_

Table 5.4. Age Preference Labels Derived from Greek Roots (Seto, 2017)

Name	Ages
Nepophilia	Infants and toddlers to ages 2
Paedophilia	Prepubescent children, ages 3-10
Hebephilia	Pubescent children, approximate ages 11-14
Ephebophilia	Adolescent minors, approximate ages 15-17
Teleiophilia	Young, sexually mature adults (ages 18-late 30s)
Mesophilia	Middle-aged adults, peri-menopausal, ages 40-60
Gerontophilia	Older adults aged 60 plus

While the previous section has explored the ages of children most at risk from online CSEM exploitation, it is also crucial to identify the gender of the children most at risk. There are several reasons for this inclusion which relate to how organisations can design and implement safeguarding measures and procedures directed towards those most at risk. Accordingly, the next main section will look at the most prolific gender of children who are identified in online CSEM exploitation.

### 5.4. The gender of children identified in online CSEM

This section explores data from the IWF, which is essential in understanding the age demographic of children most at risk from online CSEM abuse. When analysing the IWF data from 2009-2021, early data from 2009 only includes children's ages, not their gender. Also, it was not until 2011 that the IWF classified the gender of children seen in the reported content of CSEM.

Figure 5.1. IWF highlights the incidences of the female gender identified in online CSEM. Initially, the figures represent the year and percentage of female victims in online CSEM as actioned by the IWF. As a result, in 2011, the IWF identified that 65% of female children were victims of online CSEM offending, while in 2021, the Figure was 96.5%.

To place this data into some context, in 2011, there were 2,267 million Internet users globally, or 32.7% of the world population (Internet World Stats, 2023). Moreover, in 2023, there were currently 5.16 billion internet users globally, which is 64.4 % of the world's population (Statista, 2023). For that reason, it is not unsurprising that images containing CSEM will increase year on as more individuals are using the internet and smartphone technology use becomes affordable.

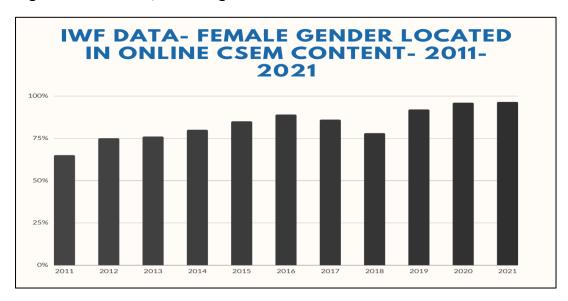


Figure 5.1. IWF Data, Percentage of Female Gender Located in Online CSEM-2011-2021

If we again refer to Figure 5.1. IWF, in 2017 and 2018, the data showed a reduction in CSEM images detected at 86% and 78%, respectively. Although only a slight decrease in 2017 (3%), the decrease in 2018 was more noticeable at (8%). This decrease in female children identified in CSEM, although less than 10%, still deserves some investigation, especially as the IWF processed more reports than in previous years.

To this end, in 2021 alone, the IWF processed 132,636 reports of CSEM, an increase of 26% from the previous year. A similar pattern was noted in 2018, where 229,328 reports were processed, an increase of 76%.

Accordingly, the reports processed by the IWF rose significantly in these two years, yet the number of female child victims decreased slightly in 2018 by 8%. Yet, the differences in these figures can be affected by several reasons. Illustrating this, the IWF claims that one report investigated by them may contain thousands of images which may affect the data. Additionally, some of these images may have been repeatedly shared and reproduced on a significant scale (IWF, 2021). Upon consideration, another possible reason could relate to more web pages containing CSEM material being produced in Europe, as opposed to North America at 48% and 44%, respectively (IWF, 2021).

This trend became apparent in 2016 when most online CSEMs assessed by the IWF shifted from North America to Europe (IWF, 2021). For example, the IWF (2021) data claim that 72% of online CSEM is now hosted in Europe, including Russia, while North America hosts 17%. Furthermore, it is noticeable that the most significant proportion of online CSEM originates in The Netherlands, with 41% of the content. On account of this, these figures may suggest that the business model of 'bulletproof hosting' can take advantage of the more tolerant legal systems and technical infrastructure provided by countries such as the Netherlands (European Commission, 2020).

'Bulletproofing hosting' is not dissimilar to usual web hosting sites, still, the companies who own them are more lenient about what content can be hosted on their servers and are found in countries with relaxed laws relating to the type of content (Norton, 2023). Despite the ease with which illegal content can be hosted on these platforms, illegal activity lies with the customers rather than the hosting site (Norton, 2023). Yet, many academics agree that while there is some customer responsibility, 'bulletproof hosting' sites provide criminals with technical capabilities resilient to criminal investigation and complaints (Arlwais et al.,2017). Bradbury (2014) illuminates the concerns of these platforms, particularly the use of online CSEM which calls for more robust measures from service and industry providers to prevent and deter the online exploitation of children on these sites.

Highlighting these issues Goncharov (2015) argues that although countries with lax legal regulations host 'bulletproof platforms', many providers explicitly state that they do not allow any hosting of CSEM. Moreover, most countries agree regarding the illegality of online CSEM and condemn this type of content, working with other organisations and law enforcement to stop these hosting services (Goncharov, 2015).

Yet, despite these claims, The Netherlands now hosts the majority of online CSEM identified and removed by the IWF. Consequently, it is reasonable to suggest that certain countries' lax regulations and laws may account for some increases in online CSEM, identified and removed by the IWF.

The increase in children identified in CSEM over the COVID-19 pandemic, 2019-2020, shows increases in the number of female children identified by the IWF. Yet after the prominent peak of the COVID-19 pandemic, when the global lockdown began to decrease, there was still an increase in the number of female children identified by the IWF (IWF, 2021). Illustrating this, in 2021, data from the IWF showed a slight increase of 0.5% in female children. Necessarily, the increase of female children identified in CSEM, although only slight, suggests a need to analyse future trends in this area to see if this trajectory continues.

Turning to the data regarding male children, the IWF has also included statistics from 2011-2021 regarding the number of reports and identification of male children identified in online CSEM. In Figure 5.2., 2011, the data appears significant, with 26% of male children identified in CSEM images. Nonetheless, the number of males identified in CSEM images decreased significantly and remained stable from 2012 to 2017, with a mean average of 10.2 %, yet one limitation of the data is that it does not explain the variation in the data set after 2012.

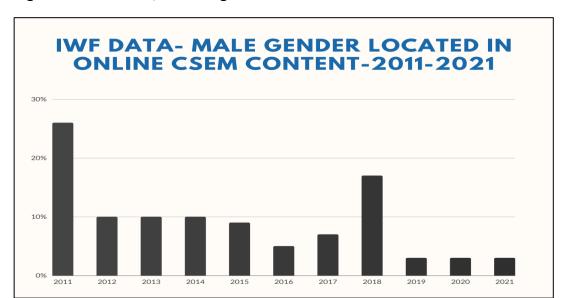


Figure 5. 2. IWF Data, Percentage of Male Gender Located in Online CSEM-2011-2021

Significantly, in 2018, the figures for male children identified in CSEM images increased to 17%. One explanation for the increase could also relate to similar outliers seen with female children in the IWF data. The data over the COVID-19 pandemic, 2019-2021, remained stable, with an average of 3% of males identified in online CSEM images. Moreover, recent IWF data from 2021 claimed that just 1% (2,641) of reports investigated depicted the sexual abuse of boys. When compared to girls, a higher proportion of CSEM images of boys (53%) depicted the most severe Category A compared to girls (17%). Yet, Figure 5.3. paints an entirely different picture of the severity level of categories of abuse within the images of boys compared to girls. Notably, the high rates of Category A images amongst boys are concerning, while Fig 5.4 illustrates that girls are more likely to be victims of Category C image abuse

When exploring the online sexual grooming of children, most attention has focused on girls rather than boys, with fewer parents concerned with online safety regarding boys when compared to girls (Fleming et al., 2006). One reason behind this claim may suggest that girls are more likely to disclose to parents online sexual abuse than boys, with boys more likely to hide any online sexual abuse (Hershkowitz, 2006; Preib & Svedin, 2008). Consequently, the IWF data is significant and should open debate for organisations and government responses to implement safeguarding measures explicitly targeted towards boys.

Figure 5. 3. IWF Data-Severity of Analysis Category of CSEM Affecting Boys-2021

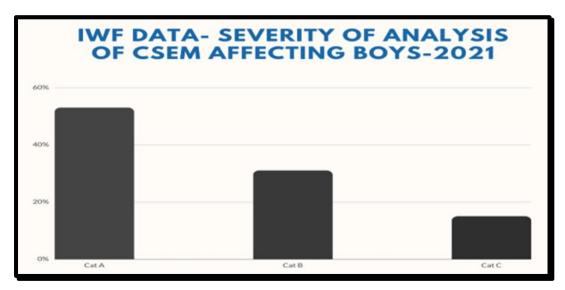
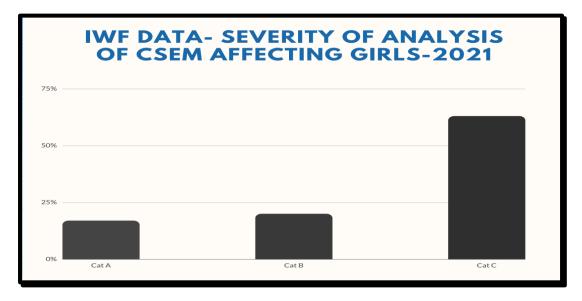


Figure 5.4. IWF Data-Severity Analysis Category of CSEM Affecting Girls-2021



As previously discussed, Category C images, although deemed less severe than other categories, are still illegal within UK law and are also damaging to the children depicted in them. Despite this, one reason for the gender differences related to these issues could relate to the propensity of girls to share self-generated images more than boys. In addition, during the IWF data collection, 76% of all images and videos containing CSEM were of girls, with the remaining 12% of boys. These differences are significant, with female children appearing most at risk, however, boys identified in CSEM images also deserve further investigation regarding why they are more prominent in the most severe categories of online sexual abuse.

To summarise, the data suggest that both boys and girls are equally at risk from online CSEM abuse, although in different forms. Notably, boys are more at risk of the most severe Category A abuse than girls, while girls are most at risk of sharing self-generated content through exploitation and coercion. It is noted within the literature that boys are not as open as girls when discussing online abuse, and this is an area which requires more work. Additionally, girls aged 11-13 appear highly vulnerable to online CSEM abuse. On this account, this thesis addresses these issues and highlights the age and gender demographic factors of the most at-risk children.

Identifying the most at-risk groups who are prone to online sexual exploitation and abuse allows practitioners and the technology industries to focus on safeguarding countermeasures and responses. Due to this, education plays a significant role in safeguarding and protecting children from online harm through appropriate intervention and guidance. Rahman et al. (2020) highlight the importance of cultivating awareness and knowledge amongst internet users early, especially in young children, to enable the safe use of cyberspace technology. Consequently, this thesis calls for age-appropriate education and guidance for children and teenagers relating to the safe use of social media and other digital platforms.

The next main section will introduce the reader to the concept of self-generated images of children. This section will then analyse the data from the IWF and others relating to the phenomenon of self-generated images of children. Understanding changes in technology and behaviours related to self-generated images is vital for effective technological countermeasures and educational responses to this concern.

Moreover, Quayle (2022) argues that children sharing self-generated content places a burden on law enforcement responses but also adds a degree of victim blaming and the criminalisation of children. Suitably, there is a need to understand this concern to add to our knowledge of what is known in this area.

### 5.5. The rise in self-generated images of children

According to the IWF (2022), self-generated images of children involve children creating naked and sexually inappropriate images of themselves using webcams, smartphones or tablets and then sharing them online via many online platforms. Also, Self-generated images are sometimes called 'sexting' (Quayle, 2020). Sexting is often seen as a way in which children and young people use online technology to understand and manage their sexuality by experimenting with sexual expression and identity and forming intimate relationships (Subrahmanyam & Smahel, 2021).

As previously mentioned, data from the participant interviews are used within this section to support the findings. Here, interviewees narrate their understanding of self-generated content.

Jennifer, civilian investigator, online child sexual crimes unit: A self-generated image would be a child that has used some form of social media application such as TikTok, Facebook, or anything like Instagram where they would upload or just create an indecent image or video of themselves.

Alan, civilian investigator, online sexual crimes unit.: So, it's people uploading to Face-book, uploading to YouTube, we do get, probably, this year, we would maybe have twenty self-generated where young people are uploading videos to TikTok and YouTube.

The definitions from these participants describing self-generated images fit the concept of our understanding of this problem and support the literature. The following quote from another interviewee discusses the legal pitfalls of sharing self-generated images:

Harry, DC, Divisional CID: And it is so easy for them to take a picture of themselves, send it to a boyfriend or girlfriend, and I do not think they realise it that when they have sent that picture of themselves, they have produced an indecent image, sent it to a boyfriend or girlfriend and distributed it, then they are in possession of an indecent image, and its all completely innocent to them.

Despite the innocent intentions of children creating self-generated content, it is still an offence to possess and share an indecent image of a child, regardless of whom the image belongs (Sexual Offences Act 2003). Even so, it is crucial to remember that young people who share naked and inappropriate images of themselves may be invested in what they perceive as a relationship and fail to recognise that they are being exploited (Child Dignity Alliance, Technical Working Group Report, 2019). Thereby, a certain degree of discretion should be used when criminal justice agencies deal with this online risk.

Quayle (2022) claims that criminalising children who share self-generated images has concerns based on their decision-making and sexual autonomy. In addition, Brennen & Phippen (2018) argue that using the term self-generated images fails to account for children sharing these images due to coercion, pressure, and extortion. Yet, despite the rights of children and young people's rights to sexual autonomy, the following quote from one interviewee makes a counterargument for a more robust response to safeguarding children and young people when sharing self-generated images of themselves:

Harry, DC, Divisional CID: Then, if it is a short video clip or picture of them and the face can be recognised, it is out there, and if it gets passed around schools, high schools, colleges or whatever, there is then that embarrassment, the stigma, and parents get to know. Before you know it, you have a child who might be having suicidal thoughts because of what has gone on.

Although Quayle (2022) highlights children's and young people's rights, the interviewee draws attention to a delicate balance between law enforcement legislation and the child's best interest. Moreover, despite the risk of criminalising children, the Internet Investigation Report (2020) states that Greater Manchester Police, recorded children as the 'primary offender' in almost 50% of indecent image cases, while Cumbria Police recorded the largest group of 'suspects' for indecent images as children. Hence, the figures related to the sharing of self-generated images by children are a cause for concern which calls for more robust safeguarding intervention and academic investigation in this area.

In response to the criminalisation of children who share self-generated content, Quayle (2022) responds by arguing that legislators should adopt policies which weigh up the protection of children against the child's integrity and privacy rights following an evidence-based impact assessment. Still, despite the many arguments within academia for the rights of young people to express themselves freely, in many cases, children are sexually groomed, deceived, or extorted into making and sharing sexual images, live streaming or videos of themselves. Consequently, it is often difficult for criminal justice agencies to know who is responsible for producing self-generated images and whether the child has been coerced, extorted, or manipulated into sharing the images.

Many children who have shared self-generated images blamed themselves, citing poor judgment and naivety, which lends itself to the current discourse on this subject (Mandau, 2021). It should be mentioned that many images shared consensually by children with friends and peers are re-shared without permission. Illustrating this, the theory of reasoned action regarding the sharing of self-generated images raises reasons for this problem. Suitably, Ajzen & Fishbein (1975) offer a framework which may explain the intentions behind an individual's behaviour to engage in certain types of conduct by exploring attitudes and perceived norms.

To support this theory, Seto (2023) argues that the theory of reasoned action suggests that young people who report favourable attitudes towards sexting and who see sexting as a standard practice amongst friends and peers are more likely to engage in sharing self-generated images.

Highlighting this, Clancey et al. (2019) argue that self-generated images shared without consent were predicted by normalised attitudes regarding the re-sharing of images. Regardless of the freedom for young people to express themselves sexually, children and young people increasingly have sexual interactions with adults or those they believe to be over 18 (Thorne, 2021).

If we compare the evidence so far from this study, sexting or children sharing self-generated images is a primary concern, not only for the children being exploited but also for law enforcement agencies that deal with these types of offences. As previously mentioned, the Internet Investigation Report (2020) has provided data where children are recorded as offenders and over 50% of referrals relate to self-generated images. These figures place police forces in a difficult position as they must identify the children involved, safeguard them, and make referrals to social services. Due to this fact, this process takes time and resources on already overstretched services.

To quantify this problem, in 2022, there were over 650,270 referrals to local authorities regarding children at risk, an increase of 8.1% from the previous year and the highest since 2019. (Gov. UK, 2022). While these figures do not tell us how many children were referred due to sharing self-generated images, the data provide a snapshot of the numbers of children requiring immediate safeguarding.

When investigating cases where children have shared images of themselves, the police service is often faced with difficult decisions regarding how they investigate these incidents. For example, Phippen & Bond (2024) point out, that although police are allowed some discretion in taking no further criminal action in cases where children had sent or shared intimate images of themselves, inconsistencies in various police forces resulted in some children being prosecuted. However, despite the inconsistencies in the investigation process, there is still a need to balance the right to sexual expression and privacy of children and young people with the overall paramountcy of safeguarding.

Children sharing self-generated images may also have other long-term negative effects on mental health and well-being. Bates (2017) claims that images shared without consent can cause long-term trauma, similar to those who have experienced domestic abuse. Moreover, Zvi & Bitton (2021) discuss the impact of images shared non-consensually, with victims blaming themselves and victim attribution by others.

Fitly, the finding from this study argues that sharing self-generated images and sexting by children and teenagers is an ever-growing concern which will continue to increase as online technology becomes more sophisticated and accessible. As such, there is a need for age-appropriate education in this area and further academic inquiry to increase our knowledge and understanding in these areas.

So far, this thesis has demonstrated that there are two facets to the sharing of self-generated images of children. One allows for self-expression, privacy and sexual experimentation of children and the other concerns criminal legislation and safeguarding responsibilities. Under the circumstances, the findings open a debate between academia and the criminal justice system over the rights of young people, their freedom of expression and safeguarding.

While there are practical responses for practitioners to address this problem by way of education for children and policing responses, the implications for scholars and academia are much more complex. Not only are there ethical considerations for academics to consider when adding to knowledge in this field, but also the responsibility to ensure that research related to safeguarding children is not only ethical but responsible

The next main heading in this chapter is related to the concerns of younger children sharing self-generated content. This thesis argues that it is crucial to learn more about the emerging trend involving much younger children sharing self-generated images. Younger children, those under the age of 10 involved in sharing self-generated images have implications not only for safeguarding and criminal justice organisations but also for academia and scholars.

## 5.6. The ages of children sharing self-generated images

Recent Internet Watch Foundation (2021) data reported that 68,000 self-generated child sexual images are uploaded yearly. In addition, data from Every Child Protected from Trafficking (ECPAT, 2021) claim that 48% of children in their study of children's every-day exposure to sexual crimes had shared nude images of themselves with others. Furthermore, in 2020, there was a 235% increase in reported self-generated imagery of 7-10-year-olds, making this the fastest-growing group (IWF, 2020).

Given these statistics, it is crucial to understand and identify the leading at-risk younger age groups sharing self-generated images.

To remind the reader, the most vulnerable and at-risk demographic relating to CSEM overall is aged 11-13. To support this theory, in 2019, the IWF found that 81% of self-generated images were of female children aged 11-13 and that most livestream abuse imagery and videos depicted children aged 11-13. Comparing these figures to similar data from Thorn (2020), the percentage of children sharing self-generated images in the 9 to 12 age group was 14%, while the age group 13 to 17 was 19%. These figures are based on Thorn's mixed-methods research, quantitative questionnaires and self-reported data from children aged 9 to 17.

Thorn's (2020) study involved 742 9-12-year-olds and 1,260 13 to 17-year-old children. When analysing the data, 103 children aged 9-12 shared nude or inappropriate images of themselves, while 239 children in the 13-17-year-old group also shared similar images. Accordingly, 342 children from a total figure of 2002 (17.08%) shared images of themselves online. Even so, it is notable that 103 of these children were in the younger age bracket, aged 9-12 who shared images of themselves.

Notably, Thorn (2020) uses the age demographic of 9-12-year-olds rather than ages 11-13, as used by the IWF. While there are benefits to the researcher using younger children in studies of this nature, there is a chance that data may be compromised by using younger children. For example, the children aged 9-12 in Thorn's (2020) study were only allowed to participate if caregivers and parents provided written consent detailing the nature of the study. This could present problems as children may not be as forthcoming knowing that their parents consented and knew of the purpose of the study.

Gallagher et al. (2010) discuss the problems of children and consent within social studies, primarily a desire to please the researcher, the consequences of not being seen as cooperative, confidentiality and safeguarding (Heath et al., 2007; Anderson & Morrow 2004). Other problems are also noted when conducting research with children and sensitive subjects, for example, some scholars note the capacity of children in the research process to make important contributions related to sensitive subjects such as alcohol misuse and domestic abuse and violence (Hill, 2015; Evang, & Øverlien, 2015).

Inevitably, children may be reluctant to share accurate information regarding their experiences of sharing self-generated images.

Upon further exploring the data from the IWF, it was noted that in 2021, they assessed 252,194 web pages containing 182,281 or (27%) self-generated images. Resultantly, 147,983 web pages involved children aged 11-13, representing 59% of all actioned reports and 89% of all self-generated images identified by the IWF (2021). These figures indicate that the number of self-generated images of children is concerning; even so, the age demographic (11-13) appears to highlight the most prolific risk age group of children involved in sharing images. The most recent data Fig 5.5. from the IWF published in May 2023 suggests that 11-13-year-olds are still most at risk from self-generated image CSEM.

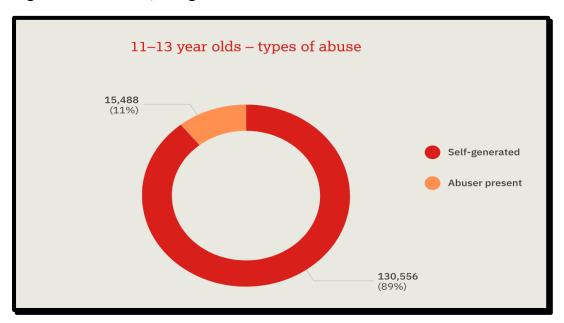


Figure 5.5. IWF 2022, Self-generated CSEM Abuse 11-13-Year-Olds

In response to this concern, Seto (2022) addresses the problem of identifying the age demographic of children most at risk of sharing self-generated images. For example, in their Meta-analysis study on sexting behaviour among youth, Madigan et al. (2018) analysed 39 separate studies on youth sexting. Regardless of using a large data set, some limitations are noted.

For example, Seto (2022) argues that within the Meta-analysis, only one study included children under 12. In addition, only two children out of 359 aged 10-12 had participated in sexting (Seto, 2022). Furthermore, the average age of the children within Madigan et al. (2018) was 15.6, in contrast to the current data from the IWF, which suggests the ages of 11-13 are the most prolific at-risk age group. Other limitations within Madigan et al. (2018) relate to the age of some studies, with a mean average publication date of 2014.

The age of these studies is significant as technology has improved and developed in the past decade, where smartphones and tablets are much more sophisticated in live streaming and image-sharing capabilities (Science Museum, 2018). Another limitation noted by Madigan et al. (2018) argued that some of the studies within their analysis define sexting as sharing sexually explicit images, videos, and text messages. In contrast, some studies define sexting as sharing self-generated images per se. Also, Cooper et al. (2016) define sexting as sharing or posting sexual content and nude images in messages and images by mobile telephones or over the internet. Thus, some definitions of sexting may vary, as sexting may include sending sexual messages (Klettke et al., 2013).

There is an important debate in the area of defining sexting and the risk to children, similar to the definitions of cybercrime as noted by Furnell (2002) where differences in the use of terminology may affect how academia and criminal justice organisations respond to these concerns. For this reason, this thesis argues that academic studies in this area should define sharing self-created/generated images or sexting clearly to provide a broader picture of the overall issues related to this concern.

This section of the thesis has highlighted concerns regarding the age and gender demographics of children sharing images of themselves online. It is accepted in the current literature that female children aged 11-13 appear most at risk for online sexual harm overall, including sharing self-generated images. Nevertheless, this thesis has uncovered some limitations in this area. If we look at data from Thorn (2020) their study uses children aged 9-10 as participants, but only with parental consent. The inclusion of this younger demographic is vital to increasing our knowledge of online sexual crime responses and how children are at risk from sharing self-generated images and sexting. Even so, this does present some problems related to future research. Recruiting a cohort with a much younger demographic presents problems related to parental consent and children not being as honest with their responses.

From a more ethical perspective, is it appropriate for researchers to expose younger children to such an emotive process which may cause more emotional distress and harm?

Despite these concerns, this thesis illustrates that the younger age demographic, those under 10, is missing from what we know about the phenomenon of online sexual crime investigation and the sharing of self-generated images. To this end, the next main heading will explore the risk to younger children those under 10 who share self-generated images.

## 5.7. Younger children sharing self-generated images

So far, this thesis has highlighted the most at-risk demographic of children and online CSEM abuse. However, this thesis has also illustrated the emerging concerns of younger children, those under 10 who are at risk of online harm and sharing self-generated content. According to the IWF (2022), there was a steep increase in self-generated images of children aged 7-10, an increase of 129% from the previous year. To this end, this section now explores this concern and notes the interview narratives in this area.

Alan, civilian investigations officer: The ones we tend to get are young children who have a mobile phone, have mum's mobile phone, and they are doing little videos. And again, young children, we have one this week; it is a young boy, maybe six, showing his bum and laughing; it is the virtual bike sheds.

Georgina, Detective, CID: I have had one (referral) where the child isn't of the age of criminal responsibility, and they have put a picture on YouTube. Also, it ended up with a completely different resolution, like the 'crime' was written off, so it was social services and school (who dealt with it).

(Parenthesis inserted by the researcher)

The narratives from these participants suggest that in this study at least, younger children than previously known are now engaging in self-generated imagery, altering the concept of knowledge in this domain. It is interesting to note that a participant claimed that one self-generated image report they had investigated involved a child under the criminal age of responsibility.

Notably, the criminal age of responsibility in England and Wales is ten, so the child must be below this age. The interviewees' narratives corroborate with recent data from the Internet Watch Foundation (2021) and the Thorne Report (2022) regarding the increase in younger children sharing self-generated images. For example, In their annual report, the Internet Watch Foundation (2021) noted that young children aged 3-6 are now uploading self-generated images and videos on many platforms. For this reason, this thesis draws attention to this area and how much younger children are now at risk of self-generated CSEM.

The younger age of children uploading self-generated images onto social media platforms is in contrast with previous academic literature in this area, which suggests that much older children, those aged 11-13, are usually involved in this behaviour. Moreover, recent IWF (2021) data also claim that self-generated images of children, aged 7-10 have increased significantly, making it the fastest-growing age group for this type of behaviour. Accordingly, the IWF (2021) conducted a study in October-November 2021, specifically focusing on self-generated content involving much younger children. Resultantly, out of the 51 reported incidents, one child was believed to be aged 3-6. Moreover, seven out of ten children in the images (69%) were aged 7-10. Due to this reason, the data suggests that much younger children are now involved in sharing self-generated images than previously known.

In their analysis of videos containing self-generated images, the IWF Annual Report (2021) summarise the content: "Some young children appear to 'perform' as if they are in a show", "and it is evident they are perhaps trying to please an 'audience" "It also appears that the children do not realise they are exploited and are seen laughing". "Other children are seen gazing into the camera, reading from a script, and showing no emotion." "In other footage, several children encourage others to commit sexual acts."

The IWF (2021) also claimed that one video contained a noticeably young boy, aged four, whose older sister carried out a sexual act on him. Accordingly, 29% of the self-generated images of 3-6-year-olds were Category A, the most severe.

The data so far suggest that our perception of children involved in sharing self-generated content has altered from what is currently known and, therefore, should also focus on much younger children, particularly those aged 6-10. Younger children involved in sharing self-generated content on videos uploaded to a platform such as YouTube may not realise that this behaviour although seemingly a fun thing to do is placing them at risk of online sexual abuse or their images being re-shared by online CSEM offenders, thus revictimising the children. Accordingly, this thesis highlights safeguarding implications for practitioners and policing organisations to address this newer emerging trend of younger children sharing self-generated content.

Leading on from this, the next main heading looks at the changes to online technology and the risks to children. Notably, as technology continues to improve and adapt at a fast pace, the online technology industries and indeed criminal justice and police agencies need to keep track of the risks to children by developing new and emerging countermeasures to this threat.

## 5.8. The changes in online technology and the risk to children

While the statistics concerning the severity of younger children sharing self-generated images are noted, there is a need to identify the possible causes. One reason for the rise in self-generated images of younger children could relate to the COVID-19 pandemic. Highlighting this issue, the IWF (2021) claim that sexual predators have exploited a rise in online activity during the COVID-19 pandemic by manipulating primary-age school children into abusing themselves on video, with reports rising by over 100%. Thereby, it could be argued that the COVID-19 pandemic has revealed our vulnerabilities to health threats and our inability to protect children from online harm (Martellozzo & Bradbury, 2021).

At the height of the COVID-19 pandemic, from 2019 to 2020, the IWF (2019) reported a 77% increase in actioned webpages displaying self-generated images of children. Moreover, the IWF (2019) suggested that these figures are representative of the lockdown and children being at home more than usual. Additionally, the IWF (2022) claims that there has been a 360% increase in self-generated images of 7-10-year-olds when compared to the first half of 2020 when the UK entered its first lockdown. While it is convenient to associate the COVID-19 pandemic with increases in self-generated images of children per se, this may not be a complete picture.

Consumer research shows that during the lockdown in the UK, 10.3 million consumers purchased new devices due to spending more time at home (Deloitte, 2020). Similarly, other consumer research suggested that global shipments of tablets in 2020 increased by 17% to reach 43.3 million units sold, its highest growth rate in six years (Chang, 2020). The digital applications used on these devices to share self-generated images and videos are essential factors to consider. Suitably, it is prudent to discuss the rise in these online services and their correlation with the increase in self-generated images.

Before the global Pandemic, individuals were moving away from text messaging and land-line calls in favour of Facebook Messenger and WhatsApp (Ofcom, 2022). Moreover, Ofcom (2022) suggests that the COVID-19 lockdown has rapidly accelerated the technological adoption of these platforms, with Facebook Messenger slightly behind Apple's FaceTime feature. Additionally, in 2020, almost all children aged 5-15 were online using laptops, tablets and mobile phones. Consequently, children's video-sharing platforms (VSP) usage was universal, especially during the COVID-19 pandemic (Ofcom, 2022). With this in mind, claiming that the COVID-19 pandemic was solely responsible for the increase in children's self-generated images requires further investigation into other aspects and potential causes. While the COVID-19 pandemic may be relevant to the increase in children sharing self-generated images, other factors should be considered.

Gabriel (2020) argues that disadvantaged children became even more vulnerable during the Pandemic and subsequent lockdowns due to time spent alone and online. Additionally, Gosh et al. (2020) posit that although children and young people may be more resistant to the physical effects of COVID-19 than adults, they may be more vulnerable to psychosocial impacts.

For example, even before the global Pandemic, vulnerable children who had experienced childhood trauma such as neglect and physical and sexual abuse had an increased risk of children experiencing child sexual exploitation (laird et al., 2020).

Yet, despite these concerns, the IWF data (2022) suggest that the younger age group, those aged 7-10, identified in CSEM, has increased by 12% after 2020, the peak of the lockdown. Recent IWF data, Figure 5.6. IWF (2022), demonstrates the significant rise in self-generated images of younger children aged 7-10. Bearing this in mind, it is reasonable to argue that the COVID-19 pandemic and subsequent lockdown may be just one of the causes for the rise in self-generated images of younger children. Still, it is also reasonable to suggest that the Covid-19 lockdown may have conditioned younger children into different patterns of online behaviour, which may have continued.

All these factors mentioned thus far may explain why there is an increase in the ages of children 7-10 sharing self-generated images although more work in this area is needed. This thesis suggests that while the COVID-19 pandemic and the lockdowns share some responsibility, other factors should be considered, including the consumer data related to the purchase of tablets and smartphones and improvements in technology related to live-stream sharing platforms, including Zoom and Microsoft Teams. Moreover, this thesis suggests that children have learnt behaviour and perceived normality developed during the pandemic related to their technology use. Consequently, this thesis suggests that it is essential for researchers to capture further quantitative data in 2024 and beyond to see if the trajectory of children sharing self-generated content will continue to increase or decrease.

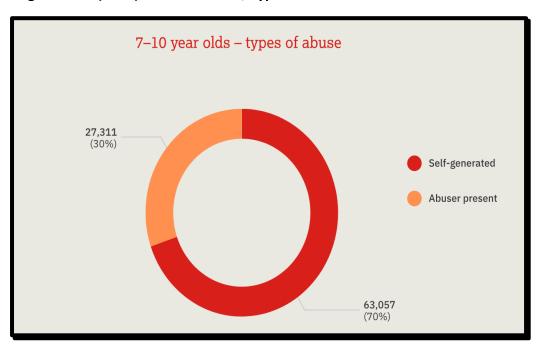


Fig 5.6. IWF (2022) 7-10-Year-Olds, Types of CSEM Abuse.

While many academic studies have explored children's mental health and well-being during the COVID-19 pandemic, there is minimal evidence as to how their online behaviours may have changed post-pandemic. Recent work by Werling et al. (2021) explored online use by adolescents with psychiatric disorders post-COVID-19 lockdown and claimed that screen and media use was reversible after the lockdown; however, online gaming did not return to pre-COVID-19 levels. Like many other studies in the genre, Werling (2021) explores the behaviours of adolescents with psychiatric disorders rather than children and teenagers overall. Appropriately, it is essential in this post-pandemic era to investigate how and if children and teenagers' online risks and habits may have changed and the subsequent consequences.

Establishing the possible causes of the recent upsurge in self-generated images is vital to implementing future government countermeasures and safeguarding responses to address this concern. While it is easy to point the finger at the effects of the COVID-19 pandemic, one must also consider other aspects, including the rise in the purchase of devices such as tablets and smartphones, the rise in VSP and children's overall vulnerability. Despite this, technology adoption relating to this phenomenon is relevant.

To this end, technology adoption and use amongst younger children and teenagers are relevant to increasing our knowledge related to the rise in self-generated content. Due to this concern, the next sub-section explores the technology used by children to share self-generated content.

# 5.9. What technology are children using to share self-generated images?

This section explores the technology children use to share self-generated images, as understanding the behaviours of children most at risk is essential for future academic investigation. Still, there is also a need for criminal justice practitioners and the technology industries to understand how children share image content to implement appropriate safeguarding procedures and countermeasures. Children now have more access and availability to smartphones, tablets, and other online devices than their predecessors. An important feature missing from the IWF data is that it does not tell us specifically what devices children use to share images of themselves.

This omission is understandable as the IWF data focuses on trends, including hosting sites, age of victims, gender, self-generated images, and commercial and dark web reports. Howbeit, despite this omission, it is important to note that 96% of children between 16 and 17 own a smartphone, while 93 % of 12 to 15-year-olds also own one Laricchia (2023). Moreover, Laricchia (2023) also claims that 27% of children aged 5-7 also own a smartphone, while the Internet Investigation Report (2020) suggests that 93% of eleven-year-olds spend over 13.5 hours per week online, with 35% owning a smartphone and 47% owning a tablet. Keeping this in mind, smartphone use among children and young people deserves further investigation into the concerns related to sharing self-generated images of children.

Today, camera-enabled devices are everywhere to such an extent that few individuals need to purchase dedicated camera devices (Hill, 2013). This claim from Hill (2013), although made a decade ago, still appears more relevant today. More recent evidence by Quayle (2022) addresses the history of camera-enabled devices by highlighting the first camera phone produced by Nokia in 2002. Initially, this device was equipped with picture messaging, a multimedia messaging service (MMS). In contrast, Hill (2013) argues that Sharp's first 'real' camera phone was produced much earlier and released in Japan in 2000. Despite the discrepancies in dates, it is accepted that most modern smartphones are the product of those earlier innovations and are now camera-enabled, which is taken for granted.

When exploring the history of sharing images, It is interesting to see earlier work by Naso (2011) when they predicted that sexting would be replaced by FaceTime, which will become a standard feature where images can be streamed from devices such as iPhones. When exploring the history of self-generated images of children they are not a new phenomenon. For example, a report by the US Campaign to Prevent Teen and Unplanned Pregnancy (2008) (NCPTUP) claimed that 22% of teenage girls and 18% of teenage boys had posted or shared nude or semi-nude images of themselves (Eraker, 2010). Additionally, NCPTUP (2008) also claimed that even greater numbers of teenagers who receive inappropriate images from friends or peers went on to share them with others. Fundamentally, this other area of online harm requires further investigation to establish the grounds and motivation for the re-sharing of intimate images amongst peers.

As evident, the concerns regarding self-generated images of children in 2008 are similar to what is seen today, with the only changes involving updated technology. If we look at the technology children use today to share images and other content, they are much more sophisticated than previous incantations. For example, Apple controls over 1.5 billion devices, the most extensive mobile telephone ecosystem globally (Apple, 2020). In addition, Ofcom (2022) claims that almost all UK children (99%) went online in 2021, with the majority using a mobile phone (72%) or a tablet (69%). Resultantly, these figures suggest that smartphone ownership and associated technologies have enabled individuals of all ages to create and share digital content that reflects all aspects of daily life (Punyanunt-Carter et al., 2018).

Notwithstanding, the technological improvements to mobile devices, there appears to be a payoff regarding the risks posed to children and young people sharing content. For example, privacy is crucial for storing and sharing sexual images with secondary accounts, such as Instagram, which are used to hide online activity from parents (Seto et al., 2023). Moreover, technology on mobile devices can enable facial recognition or other biometrics to 'open up' the device, thereby diminishing parental scrutiny.

Other ways in which children may hide their online behaviour using technology relate to the ability to create multiple profiles on social media applications. With that in mind, 6 in 10 children (62%) now have more than one online profile on specific apps, the most common reason being just for their family to see (Ofcom, 2022). Consequently, the smartphone revolution has enabled children and young people to enjoy a certain freedom and liberties not afforded in the days of the stand-alone family computer, where parents could monitor their children's online behaviour. For example, earlier work by Livingstone (2001) highlights how much technology has changed when they discuss the primary locations for children to access the internet: libraries, internet cafés and parents' workplaces. Subsequently, the ease of internet access through modern smartphones and tablets may have forever altered how children and young people interact online with peers, friends, and others.

The evidence so far suggests that much younger children are now more dependent on online technology than ever to socialise and connect with peers and friends. When analysing children's use of technology and the younger age demographic, it is interesting to see how the data from the qualitative interviews within this study compare to the IWF data. Here, interviewees note how younger children's early technology adoption, relates to self-generated images, and provide this narrative:

Interviewer: So, how is a seven-year-old managing to create or put a video on YouTube?

Alan: civilian investigator, online sexual crimes unit: Because it is second nature, they grow up with technology.

Jennifer, civilian investigator, online sexual crimes unit: Especially in this day and age, they are all using computers, aren't they? The kids are all on it as well; it is the future, and to do what they do, they have to be cyber-dependent.

When analysing the narrative from these interviewees, specific phrases are used, including "all the kids are on it" and "cyber-dependant". Additionally, one interviewee recounts what is already known, children are now digital natives, having grown up with technology. Notably, Weulen Kraebarg (2019) discusses the issue of cyber-dependent criminals who must be cyber-dependant on IT systems to commit their offences As such, despite not being criminals, children who use social media for many purposes must also be cyber-dependent and are classed as 'digital natives'.

Understanding the types of online technology children use to communicate is essential for researchers and practitioners to develop safeguarding strategies and technological safeguarding interventions. While not a new or novel concept per se, this thesis has highlighted a need for continuing academic research into this phenomenon due to the everchanging nature of technology development and the changes in technology use and behaviour of children and young people. In this vein, the next sub-heading will explore the social media applications children are using to share self-generated image content.

# 5.10. What social media apps are children using to share self-generated images?

As discussed in this thesis, police knowledge and training on social media and online digital platforms is minimal. Thus, the following section analyses the most popular social media applications children use to share self-generated images. Notably, within this chapter, the interviewees have referenced the social media apps children use to share self-generated images, namely, TikTok, YouTube and Instagram, yet they include the sites most used for the sexual exploitation of children. Table 5.5. Thorn (2022) describes the most popular social media applications children use to produce self-generated image content.

As Table 5.5. highlight, YouTube appears to be the most common social media platform children use to share self-generated images of themselves. TikTok is the second most popular social media platform children use to share self-generated images. In contrast, data from the IWF does not tell us which social media apps are being used by children to share self-generated images.

Table 5.5. Data from The Thorn Report (2022). Digital Platform Popularity of Children Who Have Experience with Self-Generated Images

Digital Platform	Children who have shared images on these sites	
YouTube	75%	
TikTok	66%	
Instagram	65%	
Snapchat	62%	
Messenger	61%	
Twitter	55%	
WhatsApp	45%	
Google Hangout	40%	
Tumblr	36%	

When analysing the data from the IWF relating to the primary sites used to host CSEM, a different picture emerges due to the lack of data relating to specific digital platforms used for sharing images. Moreover, Table 5.6. IWF (2021) details the primary sites hosting CSEM overall.

In addition, Table 5.6. does not identify which image-hosting sites are used to host CSEM nor if any of the images hosted are self-generated. Ergo, providing the reader with a brief overview is beneficial to understanding what the data represents.

Table 5.6. The Digital Sites Most Abused for Hosting CSEM. IWF (2021)

Site Type	Number of Records	% of Total number
Image host	18732	73%
Cyberlocker	24913	10%
Image Store	14621	6%
Forum	10710	4%
Banner	8086	3%
Website	2746	1%
Video Channel	2431	1%
Social Network	1104	under 1%
Search	948	under 1%
Blog	614	under 1%

As represented in Table 5.6., image-hosting sites were responsible for 73% of CSEM identified by the IWF (2021). An image-hosting service allows an individual to upload images to a remote server where the images can be viewed online. Image hosting services upload images from an integrated storage service like Dropbox, Google Drive, or Instagram (Cloudinary, 2022). Similarly, 'cyberlockers' are third-party file hosting services driven by advertisements and subscriptions. Cyberlockers provide password-protected hard drive space on devices where users can share passwords with others to share privately downloaded content (IWF, 2021).

Forum sites are a type of online message or bulletin board where interested users can share or talk about related topics. In contrast, a banner site is an advertisement displayed on a web page which consists of an image or a multimedia object (PC Mag, 2023). Notably, the remaining site types are seen in Table 5.6. relate to more commonly known digital sites, such as social media, blogs, and internet searches.

While the data from the IWF is valuable, it is also beneficial to know the primary sites used for hosting CSEM. To this end, knowing which sites are most used for hosting and viewing CSEM is essential for increasing our knowledge relating to safeguarding issues and online offending behaviours.

To finish this section, data from the current literature within this thesis suggests that YouTube appears to be the most popular social media platform children and young people use (Marsh et al., 2019; Neumann & Herodotou, 2020). Moreover, YouTube is the most popular social media site children use, with over 80% of children aged 0-7 using this platform (Marsh et al. 2020). Additionally, Marsh et al. (2019) claim that children spend, on average, 1.39 hours per day and 1.47 hours at the weekend on YouTube. Therefore, it is prudent to discuss the concerns regarding YouTube and self-generated images of children. The next sub-section will explore the concerns related to the most popular social media site, YouTube and the risks to children and self-generated images.

## 5.11. YouTube and the concerns regarding self-generated images

Despite the evidence from Thorn (2020) suggesting that YouTube presents risks to children uploading and sharing self-generated images to the site, other risk factors have been noted. Hattingh (2021) highlighted other risk factors for children who used YouTube; they noted smoking advertisements as the leading risk factor for children on the platform, along with alcohol endorsements.

Just the same, it should be noted that Hatting (2021) did not explore the risks of CSEM offending on YouTube, but rather advertisement risks, self-harm, and pro-suicide posts. Although highlighting self-harm and suicide risks on YouTube are worthy topics of discussion, the risk of online CSEMs on this site deserves equal attention.

While Hattingh (2021) highlights issues such as advertising risks to children on YouTube, it should be mentioned that YouTube is also a powerful social media platform for children uploading inappropriate or sexualised images of themselves (Thorne Report, 2022). When exploring the history of YouTube, children's viewing habits on this platform and other mass media have long been a cause of social anxiety (Garlen & Hembruff, 2022).

Such concerns later caused YouTube to introduce a YouTube Kids application in 2015, where child-friendly browsing was encouraged based on human moderators and algorithms. Yet, despite these changes, the central YouTube platform requires users to be 13 or over, which appears more popular than the younger child-friendly version.

The age verification process on YouTube and other similar platforms is concerning as there is no verification process per se related to age confirmation, just an online agreement within the terms and conditions. Moreover, YouTube remains the primary online platform for children, with 80% of them using it. Furthermore, nearly half of the children aged 8-12 preferred watching content on YouTube, while 49% of older children, those aged 12-15 preferred watching content on YouTube (Ofcom, 2022). Yet, despite the popularity of YouTube, some caution should be noted. Due to the popularity of YouTube among younger people and teenagers, the platform may be exploited by individuals for sexual purposes.

Salter & Hanson (2021) claim that CSEM offenders can upload videos to YouTube depicting children in 'revealing clothing' alongside videos of children being restrained. Moreover, the YouTube platform also links self-generated videos of children engaged in gymnastics, dancing, and swimming (Salter & Hanson, 2021). As a result, the YouTube algorithms will proactively generate innocently created self-generated videos of children for sexual predators to view online if they have previously viewed them (Kaiser & Rauchfleisch, 2019). Therefore, this is a growing concern which requires further attention from safeguarding organisations and indeed the YouTube platform itself.

To summarise this section, this thesis suggests that the literature on YouTube and the sharing of self-generated images of children are limited. Moreover, most of the literature on YouTube and the risk to children is varied and relates to viewing content, malicious URLs, self-harm, suicide, smoking and alcohol and sexual content (Neumann & Herodotou, 2020; Alshamrani et al., 2020; Khasawneh et al., 2020).

However, regardless of the evidence suggesting that YouTube is the most popular social media app used by teenagers and children, this thesis will claim that there is a gap in the literature regarding the risks caused by the rise in self-generated content on this platform, more so with much younger children, particularly those age 6-10.

Consequently, this thesis highlights not only the gaps in knowledge relating to self-generated images of much younger children on YouTube but also presses forward the responsibilities of platform providers such as YouTube and others to ensure that their safeguarding measures and technology can quickly identify inappropriate or illegal content and swiftly remove them.

This final main heading explores live-streaming CSEM abuse using video-sharing platforms. This inclusion is important as criminal justice agencies and technology industries try to understand the changes in online CSEM offending technology and behaviours which affect the risk to children.

## 5.12. What are the possible causes of the rise of live-streaming online abuse?

The recent upsurge in live-streaming offences is a primary concern for law enforcement agencies and child protection organisations. As the UK National Crime Agency reports, video cameras and video-conferencing technology have increased the risk of live-streaming child sexual abuse (The Internet Investigation Report, 2020). Moreover, data from the IWF (2018) suggest that live-streaming abuse is now a significant concern. Kloess et al. (2017) describe the ease with which offenders can interact with children, including webcam performances involving masturbation and other sexual acts. Hence, the U.K. is now the world's third-largest consumer of live-streaming child abuse (IICSA, The Internet, 2020).

The live-streaming sexual abuse of children occurs in real-time and does not require the offender to store the footage, making it difficult for law enforcement agencies to obtain evidence Thorn (2016; Europol, 2015). Also, online countermeasures such as web crawlers, CAID and text recognition cannot recognise and detect live-stream sexual abuse.

Currently, the live-streaming sexual abuse of children is affordable to the perpetrators and increasingly commonplace (Broadhurst, 2019). Due to this concern, it is vital to investigate this emerging trend to implement safeguarding measures and to increase knowledge in this area.

The live streaming of child abuse by individuals who pay others to commit these offences is usually investigated by larger organisations, including the National Crime Agency (Davis, 2020). Though there is a plethora of academic literature on live-streaming child sexual abuse, data from the IWF also provide recent quantitative data. Highlighting this, In 2018, over three months, IWF researchers examined 2,082 images and videos of live-streaming child sexual abuse and found that 98% of images were of girls aged 13 (IWF, 2019). Resultantly, the same study claimed that 96% of the victims were girls depicted in their homes.

Exploring this concern further, the National Society for the Prevention of Cruelty to Children (NSPCC) claim that offenders use credit cards to pay individuals in the Philippines to stream live sexual abuse of children for as little as £10-£15 (NSPCC, 2022). Due to this, a vast amount of academic literature discusses the concerns of live-streaming sexual abuse in the Philippines and Southeast Asia and the payment transactions (Hernandez et al. (2018; Napier et al., 2021; Cubitt et al., 2023). Nevertheless, despite the recent evidence, the Internet Watch Foundation (2017) suggests that it was now uncommon to encounter videos and images captured by live streaming to feature Southeast Asian children as they frequently encountered images involving "white girls" from "affluent Western backgrounds".

The claims from the IWF related to the changes in gender and race demographics may relate to the rise in the popularity of social media platforms where children are often sexually exploited in 'real-time', where 'live video' applications are now openly available on social media and other online platforms. This concept contradicts early work by Wolak (2015), who describes live-streaming offences where offenders pay criminals for online sexual content. While certain aspects of Wolak (2015) are still correct, new technology and existing social media applications make it easier for offenders to groom their victims and connect by video call with them on the same apps, eliminating the need for payment and organisation through third parties.

Indeed, current, and past literature suggests that coercion, extortion, sexualised grooming and exploitation are the usual methods perpetrators use when engaging with children in live-stream offending (Joleby et al., 2021; Kloess et al., 2014; Bond, 2016). Accordingly, the evidence in this thesis suggests that the live streaming of child sexual abuse has evolved and adapted to an extent where offenders no longer need to pay for live-streaming content but can access it by other means on social media platforms and live-stream video platforms. To this end, this thesis highlights an emerging concern within the online safeguarding of children and calls for further academic investigation into this area alongside age-appropriate education for the children most at risk.

Regarding the risks to children and free live-streaming services, an interviewee in this study suggests that offenders reward the children they are sexually exploiting on certain popular apps by offering virtual likes or rewards. It is well-documented how fewer 'likes' on social media posts may affect children and young people. For example, Lee et al. (2020) claim that young people who received fewer likes on social media and experienced bullying in school were the most vulnerable. Moreover, It has also been claimed that the lack of likes on social media may cause emotionally vulnerable children to use it even more to seek approval and gain positive feedback (Rideout & Fox, 2018). Likewise, previous research highlights that sharing images on some social media platforms increases social rewards such as 'likes', which may increase motivation for adolescents towards popularity (Meeus et al. (2019). Consequently, vulnerable children seeking some online approval will be at a high risk of sexual exploitation by being offered rewards on social media platforms. Here the narrative from an interviewee addresses this concern:

Jennifer, civilian investigator, online sexual crime unit: So, this is the most common thing, it is live, and it is chatting with the child directly and asking them specifically, do this for me, do that, get undressed.

The quote from the interviewee appears to support data from the IWF. Illuminating this, the IWF (2019) provide us with a case history of a seven-year-old female child who is sexually groomed via a live video call and is encouraged by an adult on the screen to perform certain acts and poses for 'likes'.

Furthermore, the child has no concept of the power of the abuser and thinks that this is just a game. Here, the interviewee provides some narrative related to 'rewards' where children are sexually abused via online games:

Jenifer, civilian investigator, online sexual crimes unit: That is why offenders are going on, saying to girls, do this for me, in the video, then they do it and reward them with these gems.

The quotes from this interviewee highlight the changes in online offending in this study from downloading indecent images to interacting live with children online. In addition, the interviewee mentions virtual rewards for children on certain gaming apps, suggesting that payment for live-streaming abuse may be unnecessary with improvements to online technology. To summarise, the phenomenon of live-streaming sexual abuse as the most recent form of child sexual abuse created by technological developments is the least investigated (Dushi, 2020).

The narrative of the interviewee highlights attention to this emerging form of online sexual offending behaviour. Moreover, data from the IWF regarding live-streaming sexual abuse of children is sparse, given their other informative data on online sexual offending. However, the IWF may face some problems in this area as live footage cannot be traced or quantified unless recorded and saved. Appropriately, this thesis calls for more investigation on this concern as it is crucial in deciding appropriate responses and countermeasures from the online technology industries and law enforcement agencies.

### 5.13. Limitations

The IWF data thus far is instrumental in increasing our understanding of changes in online CSEM offending behaviours. In addition, practitioners and academics can use the data to inform policy legislation and add to our knowledge. Yet, it would be remiss to discount noticeable limitations within the data and address these accordingly. For example, the IWF data from their annual reports are published a year behind.

Indeed, the IWF data for 2022 was recently published in May 2023. As online offending and technology develop rapidly, some data may become outdated quickly. Of course, this issue is understandable, given the vast amount of data to be captured quickly by the IWF analysts.

Another limitation in this chapter concerns the lack of clarity of IWF data regarding the digital platform offenders use to host online CSEM. By contrast, similar data by Thorn (2022) highlight the leading digital platforms used by young people and children when sharing self-generated content, which is helpful to both academics and practitioners. Additionally, more recent data by the IWF (2022) claim that in 2022, of the 255, 571 web pages actioned, 78% were self-generated images. Nevertheless, the IWF data related to the sharing of self-generated images do not always account for images shared consensually and not by sexual exploitation or coercion. Having said that, this limitation is understandable, given that the IWF use quantitative methods to obtain their data. On the other hand, Thorn (2022) uses mixed methods to obtain their data, including qualitative inquiry. As a result, a more abstract picture emerges relating to the differences in self-generated images due to coercion and sexual exploitation.

Finally, the methods used by the IWF to gather and quantify their data are unknown. It should be mentioned that the author had requested information regarding how the IWF gathered and analysed their data Appendix (D); however, this request was turned down due to the high volume of similar requests by academics and practitioners.

### 5.14. Conclusion

This chapter has analysed secondary data from the IWF relating to the following themes in order of hierarchy: The ages of children identified by the IWF data as containing CSEM; the gender of children most identified in online CSEM; the rise in self-generated images of children; the ages of children sharing self-generated images; the risk to younger children sharing self-generated content, the changes in online technology and the risk to children and the possible causes for the increase in live-video streaming abuse.

The IWF data contained in this thesis is a valuable indicator of the age demographic of children identified within online CSEM abuse material. Moreover, the increase in younger children being identified by the IWF is concerning and has several implications for intervention, safeguarding and educational responses. Under this circumstance, this thesis argues that given the current trajectory of the data, younger children aged 7-10 are at a growing risk of online harm, including sharing self-generated images. This being so, this thesis calls for appropriate education and safeguarding interventions for primary school children in online safety which is age-appropriate. On this account, it will be helpful to measure the IWF data from 2024 onwards to see if there is a predicted increase in children aged 7-10 identified as being involved in self-generated content.

This chapter has evidenced that Female children aged 11-13 have been identified as most at risk from online CSEM. Yet an interesting factor is noted when analysing the data for boys who have been identified as the most prolific victims of CSEM regarding the most severe Category A images. On the other hand, girls are less likely to feature in Category A images than boys and would feature more in Category C images. These findings are significant as girls are the most featured group in discussions and academia regarding online CSEM abuse than boys. Yet, as this thesis demonstrates, boys are equally at risk of online CSEM abuse in the most severe forms.

Proportionately, this thesis calls for specific interventions by practitioners which should be tailored to meet the needs relating to children's ages and genders. It has been claimed that younger children are now using social media platforms to share images of themselves, with younger boys specifically feeling that it is a fun idea to share videos of their bottom and private parts. To add context to this claim, one interviewee describes this behaviour as "the virtual bike sheds." Yar & Steinmetz (2019) illustrate this by claiming, that although children may view these interactions as exciting, they may also be participating in sexual exploitation by abusers who take advantage for sexual gratification. Notably, this thesis suggests that younger children are at risk of innocently sharing self-generated images without understanding the long-term implications of what they see as a fun activity.

Following on from this, how children use their social media is noted within the IWF data. A limitation of the IWF data relates to the specific digital platform children use when identified in CSEM images. For example, the IWF data claim that image-hosting sites are the most abused when locating and removing online CSEM. Yet, the data do not specify which digital platforms are the most used to host CSEM, including self-generated images. On the other hand, Thorn (2022) identifies the digital platforms most used by children to share CSEM. In this case, Identifying the specific platforms children use to share images of themselves is essential for both safeguarding intervention and research purposes.

While many studies focus on the effects of social media use, including mental health and well-being, it is essential to understand which platforms children and teenagers use for sharing self-generated images and which feature online sexual exploitation. Unsurprisingly, YouTube is also the most popular social media application for children and teenagers (Garlen & Hembruff, 2021). Given this, it is also perhaps unsurprising that data from Thorn (2022) also claims that YouTube is also the most prolific platform teenagers and children use to share self-generated images.

Despite this, It is also vital to realise that online technology is fluid, and some social media popularity may wane. For example, previous work by Hogan & Strasburer (2018) suggests that Instagram and Facebook were once the most popular social media applications for teenagers and children. But, as Clennett-Sirois (2014) points out, teenagers are not attracted to the technology itself but the affordability it provides to interact with friends and peers when there are few opportunities to socialise in person. This idea suggests that children and teenagers will use the digital platforms most suited to their needs, such as sharing images and social interaction. Consequently, this thesis calls for a better understanding and knowledge of the social media applications children and teenagers use to improve policing responses related to social media training, knowledge and awareness.

While the IWF has provided some essential data relating to online CSEM, technology use is absent. When analysing this omission, it is understandable why this data is not included, as the IWF primarily focus on trends including gender, age, and image hosting sites. The technology used by children to share self-generated content, while not essential, does create a snapshot of how children are being sexually exploited online. Essentially, learning more about the devices and smartphones children use will provide researchers and developers with possible safeguarding interventions in the future.

A final analysis of the IWF touched upon the trend in live-streaming offences. Although mentioned in recent IWF reports, the data is minimal. The IWF researched live-streaming abuse in 2018, where they analysed data over three months. However, a limitation within the IWF data relates to the original data being unavailable across all online searches. Yet, despite numerous online searches, data related to the initial IWF study is missing. Significantly, this thesis illuminates a significant area of interest in this area and argues for further academic investigation to address the balance of knowledge.

Despite the UK being the third largest consumer of live-streaming child sexual abuse, the current research focuses on payments to countries such as the Philippines rather than Western societies. The qualitative analysis within this study has highlighted the concerns of young, usually female children engaging online with strangers for sexual purposes for 'likes' and 'rewards' on gaming platforms. Previously, research in this area has focused on older children and gaming risks. Herd (2017) discusses the issues of older boys and teenagers who have been sexually groomed on online games such as Minecraft., however, minimal academic evidence relates to the live-streaming sexual abuse of younger children using online age-appropriate games for 'rewards'. Suitably, this claim has highlighted an under-reported concern in child safeguarding and questions what is currently known about safeguarding in online games designed for younger children.

To conclude, this thesis has analysed secondary data from the IWF and used interviewees' narratives throughout. This thesis has identified several issues related to existing and emerging online risks to children. While some of these issues are not particularly novel, this work has highlighted emerging and newer offending behaviours and risks to children which have previously received minimal attention. As such, this chapter has identified some significant areas of interest and gaps in knowledge which deserve further exploration and analysis.

This chapter will discuss the findings from the qualitative interviews in Chapter 4 and the secondary analysis of the IWF data and other data in Chapter 5. In addition, relevant data and findings from the literature review will also be discussed in this chapter. To remind the reader, the initial research questions asked, "Are police keeping pace with technology-driven changes in online child sexual exploitation offending?"

This question is crucial if we are to identify areas in online CSEM investigation which can help to improve the policing response to this problem and also increase knowledge in this area by way of academic exploration. To begin, the first Section will discuss the preparedness of police organisations to respond to the changes in technology used in online CSEM offending.

'The proliferation of technology has led to distinct changes in how individuals engage in the world around them'

(Holt, Bossler & Seigfried-Spellar, 2022, p.3)

## Chapter 6. The Discussion

#### 6.1. Introduction

The first section of this chapter will discuss how officers in this study working in frontline roles in online CSEM investigation and senior police leadership are prepared to deal with the changing nature of online CSEM-offending technology. As the initial research question explores police knowledge and training related to online CSEM investigation, it is prudent to discuss this issue first. It is disclosed that from the outset, this study is a snapshot of one police force and does not represent all police forces in England and Wales.

Online technology, particularly used in CSEM offending, is fluid and everchanging (Ringenberg et al., 2022). In addition, Broadhurst (2021) highlights the new and emerging technologies used in online CSEM offending, allowing individuals access to specific CSEM material to meet their needs. Taking this into account, this thesis argues that police officers face significant challenges related to the fluid nature of online CSEM offending technology and their ability to deal with this. While this claim may appear contentious given the important nature of their work, police officers and staff within this study have a certain level of training that initially may not appear to be suited to their role.

# 6.2. Are policing organisations sufficiently prepared to meet the changing nature of online technology used in CSEM offending?

The findings from the study interviews suggest that police officers and staff are trained to a high level as detectives and civilian investigators and must complete exams and meet required competency levels up to level 2 PIP (Profesional Investigation Programme). Having said that, this thesis will also argue that frontline police training in CSEM investigation lacks other essential criteria, such as social media knowledge and awareness related to the online digital platforms offenders use to groom and sexually exploit children.

Evidence by Schreuders et al. (2018) argues that frontline police officers working in cybercrime are insufficiently trained and possess limited technical knowledge. Still, the literature review findings suggest that most of the academic investigation on cybercrime and police training does not focus on online sexual crimes per se but on cybercrime overall (Cockcroft, 2018; Haddington et al., 2018; Koziarski & Ree Lee, 2020). Accordingly, this thesis argues that there is minimal academic contribution related to police training and knowledge of social media and the digital platforms used in online CSEM offending.

The findings from the literature review have also identified that specific government responses to police training related to online CSEM offending are minimal. For example, while the Online Safety Act (2023) gives organisations such as Ofcom certain powers to act against companies who do not follow the legislation by fines of up to £18 million, no mention is made of the policing responses to the problem of online CSEM (Gov. UK. Online Safety Bill, 2022). In addition, FOI requests (Appendices, A, B and C) related to other major police forces in England used within this thesis show the differences in how and what training police officers receive in online CSEM investigations.

Some police forces who provided FOI requests claimed that their officers engaged in frontline CSEM investigations had received detective training, image grading training and the Specialist Child Abuse Investigator Programme course (SCAIDP), while others had not. Interviewees in this study were trained detectives and had image grading training but not SCAIDP. Given this, the findings of this thesis suggest that police responses to CSEM investigations in England and Wales are inconsistent in some areas regarding officers' training, knowledge, and qualifications.

To explore the theory of police training responses to online CSEM, earlier work by Yar & Steinmetz (2019) claims that policing responses to cybercrime have often been criticised for being "piecemeal and inadequate" and subject to several challenges and barriers that often prevent a robust response to the vast array of internet-enabled offences. Moreover, the literature review findings also suggest that police responses to cybercrime typically focus on theft, fraud, stalking and harassment. Accordingly, this thesis supports the argument that all officers employed in online CSEM investigations should have a standardised approach to training, knowledge, and qualifications.

The literature review and interview findings suggest that policing responses to cyber-crime and online CSEM investigations should include police officers' knowledge and training related to their specific roles. For example, interviewees in this study are trained to a certain level to meet what is perceived to be their operational needs. As previously mentioned, the training for the participants in this study includes holding detective status and image grading training; yet findings from the literature review and participant interviews suggest that these qualifications alone may not adequately address the long-term problem of technological developments in online CSEM investigation and offending behaviours.

To support this claim, some interviewees in this study were candid when narrating the skill levels of their colleagues in using online technology and social media. For example, the words 'technophobe' and 'Luddite' were used by interviewees when describing their colleague's levels of online technology skills and knowledge. Compared to their colleagues, the participants making these comments could be regarded as 'technophiles' or enthusiastically embracing newer technology (Fox, 2018). These claims are perhaps unfair to the participants, given the complex nature of their role, yet they highlight the differences in operational knowledge of some officers when compared to some of their colleagues.

The suggestions made in this thesis relating to the differences in police knowledge and training are demonstrated by the narrative from the interviewees when they talk about police suspect interviews and a lack of knowledge relating to social media applications. For example, one interviewee claims that without the full knowledge or understanding of how the TikTok application works, it is difficult to understand whether somebody is telling you the truth.

As the literature review findings suggest, police suspect interviews are an integral part of police investigations and knowing about the subject matter beforehand is essential to the investigation process. Therefore, the theory of knowledge and training for police officers working in online CSEM investigations should be a formal learning process of capturing, retaining, and sharing knowledge.

Regarding image grading training, the interview findings suggest that image grading training was a contentious issue among participants. From FOI requests (Appendices A, B and C), it appears that image grading training is a requirement for all officers and staff engaged in online CSEM investigations. However, from the interviewee's narratives, image grading is a subjective process with issues primarily related to Category C images. Additionally, the interview findings suggest that Category C images are sometimes used as a yardstick for investigation priority rather than their purpose as a sentencing and charging tool.

Thus far, the findings have suggested that knowledge and learning related to the interviewee's roles fail to capture, retain, and use knowledge effectively. Regarding learning and knowledge, the interview finding also suggests that officers 'learned from each other or 'learned as they went along'. The narrative from these participants could suggest that some officers in this study relied on more informed colleagues as informal and unofficial tutors when learning about online technology or social media applications. Due to this concern, this study has identified a gap within research into this subject and calls for further academic investigation into this area involving other major police forces engaged in online CSEM investigations.

The research findings in this area support other work by Scheruders et al. (2018), who argue that police training related to cybercrime and digital support should be bespoke and include child safeguarding. In addition, the Home Office Policing Strategic Requirement (2023) recommends that police forces retain and maintain child abuse investigation units, which should be staffed by officers and staff who have undertaken the relevant specialist training to respond to cases of sexual abuse.

Even so, while the Home Office PSR document makes several outcomes and capacity requirements relating to child sexual abuse investigation per se, the literature review and interview findings suggest a need to integrate physical child sexual abuse and online CSEM offending as one entity rather than two separate issues. In this context, this suggestion is valid because officers and staff in online CSEM investigations should be skilled in all areas of child abuse investigation.

When exploring the narrative from the interviewees, the interview findings support the argument, that online CSEM offenders are now offending in all aspects of child abuse, including online offences such as possession of indecent images and physical sexual abuse offences. Notably, this thesis introduces amendments to Krone's (2004) typology of offenders which takes into account the use of newer technology in child sexual abuse offending. Table 6.1., 'complex offenders', now includes live-streaming offenders, those using virtual reality (VR), sexualised chat with children and indecent image offenders who engage in all other aspects of online offending. In addition, complex online offenders would also include a peer-to-peer sexualised chat with other individuals and grooming offenders who wish to meet with a child for sexual purposes. This concept is an important addition to the current knowledge related to online CSEM offenders as it suggests that as technology has adapted, so have the offenders. In light of this, it is appropriate to expand on this idea by way of further investigation in this area and future research.

Table 6.1. Complex Offenders. Amendments to Krone (2004) Typologies of Offenders

VR and Live stream:

Uses VR technology, webcam, or live platforms including social media apps, Messenger, Skype,
Teams and Zoom, Etc.

Complex Offenders:

May use a variety of online offending behaviours,
Including live -stream, VR, sexualised chat with
children, sharing Images, grooming to meet a child
for sexual purposes, peer-to-peer sexualised chat
with other adults and digital creators who use
software to create images of children and anime
related to child sexual exploitation and abuse.

The literature review and participant interviews also noted issues related to interworking and collaboration with other organisations. For example, in the interview findings, some participants claimed that the NCA differed significantly from their policing role. In contrast, others agreed that work experience with their NCA counterparts was a good idea. Yet, the literature and participant interviews have highlighted professional rivalry between police officers and other non-police agencies, such as the NCA, related to the civilianised role of some of these organisations.

In this respect, this thesis suggests that due to their specialised roles related to online CSEM offending, police officers involved in online sex crime investigation would benefit from work experience with their NCA counterparts and vice-versa.

Concerning training and knowledge, the interview findings suggest that interviewees valued their working experience over formal qualifications. For example, the word 'experience' appeared more times within the qualitative interviews than any other phrase. Be that as it may, the interview findings suggest that although experience is a crucial aspect of learning and knowledge, any experience gained is not retained or shared appropriately within the working environment or organisation. Considering this, the findings within this study have noted significant changes in online offending behaviour, which were not being shared or retained by policing leadership with academia or within other safeguarding organisations.

The findings from the literature review and the interviews have also identified no formalised means for officers and staff to record or share knowledge through their gained working experience. The omission of sharing new knowledge is essential for how police organisations react to the growing problem of online CSEM investigations. For example, this thesis will claim that interviewees in this study have observed significant changes in online offending behaviour, including how offenders now offend across all forms of child abuse and younger children becoming involved in sharing self-generated images consensually. In this case, this thesis argues that omitting these significant changes in offending behaviour and emerging risks to children is detrimental to our knowledge of current CSEM offending.

In support of the argument related to the sharing and retaining of new offending behaviour, past literature suggests that most offenders do not cross over or evolve from online-only offending to physical contact or dual offending. This claim contradicts the findings from the interviews in this study where the interviewees now suggest that individuals are offending online across all theatres of child sexual abuse behaviours and not restricted to one or two particular offending traits. Resultantly, this thesis argues that these critical changes in offending behaviour are not being recorded or shared with interested parties to increase our knowledge and awareness of this phenomenon.

On this account, this thesis will argue that policing leadership should have in place structured methods for sharing and retaining knowledge gained through the experience of working practice by appropriate use of learning theories, concepts, and research.

The findings from this thesis also suggest that learning theories should be employed by police leadership to capture changes to offending behaviour and to put in place policing responses to these changes. If we look at the findings where interviewees learn from each other,' a constructivist approach to theory may be considered. Also, this thesis suggests that learning theories should be adopted by police organisations involved in frontline CSEM investigations as an ongoing process of converting experience and working practice into knowledge. But, regardless of the learning theories most appropriate for improvements in service delivery, this study will argue that police leadership should consider implementing a system where knowledge is shared and used to its fullest potential with academia and other organisations.

It is important to note that each police force in England and Wales is run independently, which makes policy changes difficult. For example, Gillespie (2019) points out that the 43 UK police Forces have operational independence and territorial limitations and are responsible for investigating crime in their geographical areas. Consequently, a limitation in adopting learning theories by senior police leadership relates to the political accountability for these police forces as the local responsibility of a police force sits with the crime commissioners (Caless & Owens, 2016). Accordingly, this thesis has identified a more significant issue related to overall police training which involves significant changes to local and government accountability.

In response to the interview findings thus far, this thesis suggests that some interviewees within this study are not as proficient as some of their colleagues in their online knowledge of social media and digital platforms. Also, some interviewees cited the many social media and online digital platforms as barriers to their learning and knowledge of online sexual crime investigation. These claims suggest that some police officers in this study at least are not as confident in their knowledge of online CSEM offending relating to the technology and applications used by offenders. Resultantly, police officers working in online CSEM investigations should be expected to have a higher-than-average knowledge of social media and other digital platforms used in online CSEM offending.

Surprisingly, the interview findings within this study related to further training needs lacked ideas from the interviewees as to which areas were beneficial to them. The lack of training ideas from the participants may suggest that interviewees are unsure of their training needs related to their roles. Also, the interview findings suggest that a specific area of further training related to intelligence interviews of suspects was needed. Indeed, this thesis claims that conducting intelligence interviews is carried out in most police volume crime investigations; however, this did not occur as a routine within this study cohort. Notably, as Burton & Revell (2018) argue, enabling practitioners to call on their professional curiosity is a complex issue that may be linked to the emotive subject of a child abuse investigation. In this regard, the findings related to intelligence interviews in CSEM investigations have opened a debate for academia and for police leadership to improve working practices when interviewing suspects arrested for CSEM offences.

A final note regarding this section should focus on official accreditation for officers working in online sexual crime units. It was noted that participants in this study have two main criteria for working in online CSEM investigation: detective status and image grading training. It should be noted that the literature review suggests that accreditation in the police is related to specific roles, such as financial investigators. Yet, there is an argument which suggests that image grading training for officers working in online CSEM investigation could be viewed as accreditation, however, despite this, overall, police officers' roles in serious crime investigations involving protecting and safeguarding children should involve official accreditation (Stambaugh et al., 2001).

The next main heading will discuss how technology companies contribute to online CSEM investigation, prevention, and detection technology. This inclusion is vital in our understanding of CSEM investigations and the policing responses as technology and online CSEM offences are fast-changing and fluid.

## 6.3. New oil? Are technology companies now the primary responders to online CSEM offending?

When discussing the literature on online CSEM offending, the primary subject usually refers to offenders' typology and behaviours. As expected, much academic research already exists on offending behaviours, typologies and psychological theories related to online CSEM offending (Tener et al., 2015; Klein & Bogaerts, 2020; Henshaw et al., 2017; Aslan et al., 2014). Yet, despite this evidence, this thesis argues that the extent of existing literature on the technical behaviours of online CSEM offenders is limited (Steel et al., 2023). Suffice it to say that before we invest in criminal justice and policing responses, there is a need to create effective technical countermeasures to identify and remove online CSEM.

Periera et al. (2021) suggest that the technology industries are a vital tool in the global fight against identifying and removing online CSEM offending. To support this claim, many organisations, including Google, Microsoft, the IWF CEOP and NCMEC, have responded to this challenge by creating technological countermeasures against online CSEM offending. While Holt et al. (2022) describe this system as a complex hierarchy of organisations, it is evident that online CSEM offending relies on numerous national and international organisations' technological responses. For example, it is noted that police alone cannot tackle the problem of online CSEM and often lack the knowledge and technological capabilities to deal with this concern (Boes & Leukfeldt, 2016; Bond & Tyrell, 2018). In that regard, this claim becomes more relevant as law enforcement agencies across the globe investigate millions of CSEM cases annually (Pereira et al., 2021).

When discussing the volume of online CSEM offending, Lee et al. (2020) argue that quantifying the level of online CSEM is an almost impossible task, as new material is added continuously. In response to this, the technology industries have developed countermeasures which have been developed by industries, including PhotoDNA, web crawlers, PhotoDNA for video, and text recognition and the Child Abuse Image Database (CAID). Even so, despite the technological interventions, understanding how offenders use online technology is helpful to police as it can shape the investigation process and deter offending (Steel, 2021).

Resultantly, the work within this thesis moves this discussion forward by suggesting that without the use of the technology developed and provided by industries, police forces face significant barriers to detecting and arresting suspects involved in online CSEM offending.

Let us first look at the policing perspective as an example of responses to online CSEM offending. The literature review and interview findings within this thesis suggest that while the police are highly efficient in arresting and interviewing suspects accused of CSEM offending, other responses to this problem appear limited. For example, police online sexual crimes units do not routinely use technology afforded to other specialist policing units, such as digital forensic examiners who interrogate devices seized from suspects to search for evidence. Within this context, the evidence in this thesis claims that front-line officers working in online sexual crime units rely primarily on existing technology for referrals and evidence-gathering.

Exploring the literature in the thesis and the qualitative interviews has also demonstrated that the UK police service routinely relies on online CSEM referrals from other non-policing organisations, including the National Crime Agency, via NCMEC and other NGOs. As a result, this thesis supports the argument that most online technological policing responses to CSEM offending are now carried out by non-police organisations in the private sector, charities and voluntary sectors (Yar & Steinmetz, 2019). While it is perhaps a strange concept to suggest that police are not the primary stakeholders in online harm prevention and detection, one must explore the reasons behind this claim.

Bursztein et al. (2019) argue that online CSEM on the internet has outrun the capabilities of criminal justice agencies and other organisations to respond to this global problem effectively. In addition, the literature in this thesis suggests that the large volume of online CSEM offences places a significant burden on police service. This claim is supported by the IWF secondary data analysis in Chapter 5, which argues that every two minutes, the web pages assessed by the IWF depicted a child being sexually abused. Consequently, the exploration of the literature in Chapter 2 argues that society is now more reliant on organisations in the private sector, such as the IWF and Industry, to provide robust technological responses to online CSEM offending.

Thus far, the literature review contained in this thesis suggests that organisations, including the IWF and NCMEC, are now at the forefront of CSEM identification and disruption rather than the police. This thesis will argue that this claim is justified, given that the increase in online crime problems has stimulated the growth of external organisations, such as the IWF, tasked with monitoring the internet for illegal content and removing such content (Yar & Steinmetz, 2019).

In essence, this thesis also suggests that the technological advancement of online CSEM and the intervention of the technology industries have relegated the police to a supporting role in online CSEM offending detection, arrest, and removal. While this claim may be contrary to the public perception of police CSEM investigation, these claims are not without supporting evidence. For example, the literature in Chapter 2 suggests that the police use of technology to detect and disrupt online CSEM is limited compared to other non-police organisations. Still, this is not to say that police do not use technology to investigate CSEM offending. For example, it is noted in the literature that undercover police officers deploy online posing as children to detect online CSEM offenders. In addition, police use technology to monitor peer-to-peer chat sites and file-sharing platforms in a limited capacity. But, as the literature suggests, the scale of these interventions is nowhere near the size and capabilities of the technology industries when employed in online CSEM detection and countermeasures.

As the findings within the literature review claim, PhotoDNA, developed by Microsoft, is one of the primary technologies used by police to detect and remove known child abuse images. Indeed, Microsoft licences PhotoDNA and PhotoDNA for video free to many safeguarding organisations, including the IWF, NCMEC, and the police (Microsoft, 2022). Because of the contribution from the online technology industries, this thesis argues that without this technology, it would be almost impossible for law enforcement agencies and other non-police organisations to identify and take down known CSEM images.

On the other hand, while technology companies and other non-police organisations are at the forefront of assisting law enforcement agencies in detecting and removing online CSEM, some barriers are preventing future technology developments. As the literature findings suggest, the lack of available CSEM data sets for industries prevents the development of algorithms to identify CSEM images.

In response, law enforcement agencies appear unwilling to share live data sets due to the legal implications of sharing these images (Yiallourou, 2017; Vitorino et al., 2017). Ergo, this thesis argues that although the technology industries appear to be the primary technological response to online CSEM, they are somewhat hampered legally by their inability to create and develop new algorithms to enable effective research by the lack of live CSEM data sets.

To support the sharing of CSEM data sets, Açar (2019) argues that researchers should collaborate with law enforcement agencies to test their new algorithms. Moreover, the results of sharing CSEM data within organisations have proven to be more reliable when compared to the results from researchers who used less accurate and 'illegal' material (Sac-Bae et al., 2014). Under the circumstances, the findings within the literature support this thesis's argument for a secure global depository to share CSEM material with other law enforcement agencies and tech industries to create effective countermeasures and detection responses.

To summarise, the findings within this section have suggested that the technology industries are the primary technological response to online CSEM rather than the police. While the police play a significant part in arresting suspects and bringing them before the courts, they cannot function without the assistance of the technology industry. When exploring the literature, this thesis also argues that the tech industries require access to live data sets of CSEM images to improve their development of online CSEM countermeasures. Despite this, some problems exist, including maintenance costs and security and resource problems. By this account, this thesis will argue that despite some concerns, a single secure global repository of live CSEM images is one solution to this problem.

Suffice it to say that to tackle the global problems of online CSEM effectively, law enforcement agencies, the technology industries and other organisations should work collaboratively to eradicate online CSEM material. Furthermore, the findings within the literature review would also suggest that online CSEM offending is an ongoing and ever-evolving problem that will test the capabilities of police and technology industries. Hence, this thesis argues that technological countermeasures and responses must continuously develop to keep up with emerging trends in online CSEM offending.

The following section will discuss the secondary data from the IWF and the qualitative interviews. In addition, this section will discuss how technological, health and social developments over time have changed children's online behaviours and risks.

## 6.4. How changes in technology have affected the online risks to children

Internet-based technology and artificial intelligence (AI) are poised to fundamentally change the structure of policing and other industries (Rowe, 2020). While changes in technology may alter how the police service operates, this thesis argues that there is a need to understand how changes in technology have affected the online risk to children. For example, the literature review within the thesis supports the theory that the rise and development of smartphone technology and the COVID-19 restrictions during the pandemic may have increased the online risk to children. Notably, this thesis argues that camera phone technology has vastly improved from its conception in the early 2000s and sales of tablets and smartphones have increased significantly during the height of the COVID-19 pandemic. From this perspective, this thesis suggests that all these facets collectively may have added to the online risk to children.

Although the risk of self-generated images of children has been an ongoing concern for many years, the combination of the COVID-19 pandemic and the increase in smartphone use has created a 'perfect storm' for an increase in the risk to children when online. As a result, children and young people became more dependent on smartphone use during the COVID-19 pandemic, mainly due to social isolation (Zhen et al., 2021). In this case, the findings within the data support this thesis's claim that the dependency and increased use of smartphone devices may have encouraged certain online risk behaviours in children during the COVID-19 pandemic, which are still evident today.

To further support this claim, the IWF data explored in this study has shown that over the COVID-19 Pandemic in 2021, the number of children identified in CSEM increased to 68%. Yet, the IWF data will claim that as the pandemic restrictions were lifted by 2022, 11-13-year-olds identified in online CSEM had fallen by 10%.

These figures are expected as children are no longer restricted to social isolation as COVID-19 restrictions have been removed, however, the IWF data will also claim that while the most at-risk group of online CSEM are 11-13-year-old females, much younger children are now identified in online CSEM. As a result, in 2022, the number of children aged 7-10 identified in CSEM by the IWF, including self-generated images, has increased by 13%.

Consequently, the IWF data support some findings from the qualitative interviews in this study, which suggest that much younger children are now engaged in online risk behaviours, including sharing self-generated content and conversing with coercive adults through online games aimed at pre-teen children. To add weight to this theory, one Interviewee in this study narrates their experiences of younger female children being sexually exploited in online games by adults for likes and rewards. Nevertheless, despite the significance of this claim, it is representative of one police force and does not cover the whole of England and Wales.

The IWF data in this thesis also claim that younger children, especially boys, feel that sharing images of themselves is a 'fun' experience and, as one interviewee within this study calls, the 'virtual bike sheds'. This claim also supports the IWF data, highlighting the concern of younger children, those aged 3-6, using social media platforms to share self-generated image content. As a result, the findings within this thesis will argue that a much younger age demographic and those aged 3-6 should be the focus of age-appropriate safeguarding interventions, academic study, and education.

In addition to the risks to younger children aged 3-6, the IWF data claims that the younger age group, those aged 7-10, is the fastest-growing group of children most at risk of online harm. The IWF data and the interview data in this study have challenged the perspectives of what is currently known about children's ages related to the risks of online CSEM. Although it is accepted within the IWF data that older female children, those aged 11-13, have been identified as the most at-risk group of online CSEM exploitation, the IWF data and interview findings will also argue that a much younger demographic is now involved in self-generated image content often unreported within academic and grey literature.

When further exploring the gender of the children most at risk of online harm, the IWF data will claim that it is generally accepted that girls are primarily the main at-risk demographic. This claim is also supported by other organisations who argue that globally, one in every four girls will face sexual abuse compared to one in six boys (YWCA.org, 2017).

The findings in the IWF data will claim that although girls are seen as the most at-risk group for online CSEM exploitation, boys are the most at-risk group identified in online CSEM in the most severe Category A group. In addition, the IWF data will also claim that the number of boys identified in the most severe categories of images has risen from 17% in 2020 to 20% in 2022. Notably, the findings from the analysis of the IWF data in this thesis support the argument that post-pandemic academic investigation surrounding boys and their online risk of CSEM requires further attention.

The findings from the literature review also suggest that the concern of younger children creating self-generated content on YouTube is a relatively new and unexplored concept. Yet, YouTube is seen as one of the most popular digital platforms children use, with 80% using it (Ofcom, 2022). In addition, other data sources from Thorn (2022) related to YouTube and the risk to children were analysed to investigate this concern further. Considering this, the data from Thorn (2022) suggests that YouTube was the leading online platform children used for sharing self-generated images.

Notably, the data from Thorn (2022) echo the narrative of an interviewee in this study, who describes how younger children can easily create content on YouTube and upload the video without their parent's knowledge. As a result, the findings within this thesis support the theory that much younger children using social media platforms such as YouTube to share self-generated images are relatively unknown and require further investigation. In this context, the findings also suggest that although YouTube is immensely popular with children, there is minimal academic evidence concerning the risk to children and self-generated images when using the platform.

The current literature suggests that most academic studies on YouTube focus on other online risks, such as smoking, alcohol, eating disorders, self-harm, and other sexual content, rather than sharing self-generated images. This omission is important as it high-lights a relatively unreported risk to younger children and their social media use. For this reason, this thesis supports the idea that further research is justified concerning the risk factors of younger children related to sharing self-generated images on the most popular social media platforms.

In addition to the rise in self-generated images of children, the findings from the IWF data analysis suggest that live-streaming CSEM abuse of children is increasing rapidly. While the findings from the IWF data highlight the issues of live-stream sexual abuse of children, this thesis will also suggest that minimal data exists to quantify the extent of this problem. The findings from the IWF data and the literature review contradict our current understanding of this issue. For example, other academic literature primarily focuses on the issues of children from South Asian backgrounds who are exploited through payment methods (Cubitt et al., 2023), however, the data from the literature and IWF data analysis will claim that most live-streaming abuse uncovered now involves predominantly "white girls" from "affluent Western backgrounds".

To support the literature, the findings from the IWF provide a good idea of the country of origin where live-stream footage was uploaded and the age and gender demographic of the victims. Moreover, the findings from the IWF data analysis also highlight other factors related to the rise in Western children being sexually exploited in live-stream footage. For example, when analysing the IWF data and literature, this thesis suggests that the rise in popularity of live-chat social media applications during the COVID-19 lockdown may have contributed to increased live-stream abuse of children from Western backgrounds.

In support of this theory, data from Thorn (2022) related to their study into online grooming risks to children's and adolescents' online behaviours and social relationships during the COVID-19 pandemic were analysed. Of the 1,200 participants in Thorn's study, 26% engaged with individuals via live stream, videos, or images. Also, the data from the literature and IWF findings claim that the popularity and use of live video conferencing tools such as WhatsApp, Messenger, Zoom and Skype during the pandemic lockdowns have changed how some individuals target children and young people for online CSEM abuse.

It is now commonplace for individuals to use free online video conferencing platforms as they are a convenient and cheap method of communication. Nevertheless, it is now accepted that some individuals will exploit this by abusing children locally rather than paying for live-stream content abroad. For example, the IWF data analysis suggests that when online, children are often encouraged to move to a private conversation on live video platforms by someone they had met online on social media platforms.

Suitably, the gap in academic knowledge and the literature regarding this concern is noted in this study. The next main discussion section will focus on the changes to online and digital technology and their effects on CSEM offending behaviour.

## 6.5. How changes in technology have affected online CSEM offending behaviour

When discussing how technology has shaped and evolved online CSEM offending, the literature review findings claim that current research has failed to catch up regarding this concept. Technology changes have now offered CSEM offenders more choices to engage in deviant online CSEM offending behaviours (Quinn et al., 2004). Previously, the literature has suggested that online CSEM offenders fall into various categories, which include collectors, traders, groomers, browsers, trawlers, and producers (Hartman et al., 1984; Alexy et al., 2005; Sulivan & Beech, 2004; Lanning, 2001; Krone, 2004). Yet on the contrary, interview findings within this thesis suggest that online CSEM offenders now engage in all aspects of CSEM offending, including online and physical sexual abuse.

The literature on the typologies of adult-initiated child sexual offending is vast and dates back many years. In addition, much of the previous work in this area has focused on behavioural issues such as age, demographic and social characteristics (Goodwill et al., 2016; Saramango et al., 2020). Also, other issues discussed include personality traits such as low self-esteem, poor social communication, and general vulnerability (Terry, 2006). In this vein, the interview findings argue that when exploring the concept of CSEM-offending typologies, it is crucial to understand how online behaviours have altered to meet the need for 21st-century technology.

The findings in this study suggest that individuals who engage in online CSEM offending behaviour are no longer restricted to one specific type of behaviour but rather engage in all forms of online and offline CSEM offending. For example, the Interviewee's narratives claim that suspects no longer behave in a specific way when offending online, such as downloading or sharing indecent images, yet they are now engaging in online sexualised grooming, physical child sexual abuse, sharing and possessing indecent images of children, live-stream abuse, and sexualised chat with children. As a result, this thesis will suggest that as online technology has changed and developed over the years, so have the offending behaviours of individuals who engage in CSEM offending.

It is also important to remember that while developments in online technolgy have changed offending behaviours to some extent, these crimes are still committed by people who happen to use technolgy. Accordingly, some may see this as a problem which can be solved by using technology countermeasures and detection methods. However, as Phippen & Bond (2024) posit, online harm legislation in particular the Online Safety Act take for granted in some respects that online CSEM offending can be prevented using technology itself; however, there is a failure in some parts to view online harm offending as a societal concern rather than a purely technical one. To this end, to counteract online CSEM offending behaviour, there must be a recognised association with the offenders themselves as individuals and their use of technology.

Findings from the literature review suggest that two types of online CSEM offending behaviour coexist alongside previously known CSEM typologies. For example, 'virtual reality (VR) and live-stream offenders and 'complex' offenders should also be considered. Table 1.6. highlights these newer types of offending behaviours and also the methods used. For example, VR and live-stream offending now encompass changes to online technology, including instant messenger apps, facetime and video call software, Zoom, WhatsApp, Facebook Messenger, Microsoft Teams, and Google Video Call. Properly, this thesis argues that as online technology has evolved and adapted over previous years, so has online CSEM offending behaviours and the increased online risk to children.

As Dushi (2020) argues, live-streaming sexual abuse is the most recent form of child sexual abuse and the least investigated. More recently, Cubitt et al. (2022) identified a subgroup of live-stream offenders who engage in contact sexual offending. The claims from Cubitt et al. (2022) appear to support the findings in this study, which suggests that CSEM offenders are now engaging across all aspects of online CSEM offending. Using this interpretation, this thesis argues that understanding the changes in online offending behaviour is essential to increasing academic knowledge and developing technology countermeasures and proactive responses to this global problem.

Still, despite the usefulness of identifying new offending behaviours, some suggestions claim that placing offenders into typologies or labels creates more problems than solutions, particularly where treatment and therapies should be prioritised (Schwartz, 2011). Despite this criticism, this thesis argues that it is crucial to identify new and emerging types of online offending behaviours regarding the risk to children. Due to this, the interview findings suggest that there is now a challenging argument for exploring the changes in online technology that affect how individuals engage in online CSEM offending.

Against this background, the findings in this study argue that live-stream video CSEM abuse has changed from what was previously known about this phenomenon. Viewed in this way, this thesis identifies weaknesses in current academic studies and investigational approaches to the problem of online live-stream abuse and the risk to children. To summarise, this thesis argues that as online technology changes and adapts, so does the behaviour of those who offend and who use the technology to offend. Finally, this thesis suggests that the emergence of the 'complex offenders' theory deserves further attention through qualitative academic study with practitioners who engage with online CSEM offenders.

#### 6.6. Limitations

Although the topics mentioned in this discussion chapter are appropriate, some limitations are noted. One limitation previously mentioned in this study relates to the use of one police force rather than several. It would have been highly beneficial to include the narrative from participants in other police forces related to the current themes, but it should be considered that the author did contact other police forces regarding the study alongside the NCA, who did not wish to participate in the research.

Another limitation relates to the interview cohort's lack of middle and senior management. Using middle managers in the interviews may have provided more findings regarding issues related to knowledge, training and learning theories. Again, the author attempted to engage middle and senior managers without success.

As with most secondary data analyses, some limitations exist. While the data from the IWF is instrumental in depicting the level of self-generated images of children and other concerns, the IWF data surrounding live-streaming offending is minimal. Moreover, the IWF (2018) data study into live-streaming offending has been removed from their web pages and associated links. Given this, only an overview of the data from this report currently exists. Yet, given the rigour of the IWF usually employed when analysing and discussing their data, it should be trusted as accurate.

Another limitation relating to the IWF data is concerned with how the IWF gather and analyses its data. How the IWF obtained their data, or the methods used to analyse it is unknown to the researcher. The researcher applied to the IWF to see first-hand how they collected their data, but this was impossible due to the large volume of similar requests they receive annually (Appendix D). It should be noted that the IWF states that trained data analysts gather their data from various sources. Subsequently, it is widely accepted by various organisations and the UK government that the IWF data is robust and accurate.

### 6.7. Implications for policy and practice

This chapter will finish by highlighting how the findings in this thesis may influence policy and practice in real-world applications and future research. It is noted that much younger children now have more unsupervised access to smart devices such as mobile phones and tablets than their counterparts in the 1990s and beyond. The advanced technology of these devices enables live chat facilities across several digital platforms and social media. Where education and parental intervention for this age demographic were once minimal, there is a strong need for age-appropriate interventions for children under the age of ten years. Accordingly, as Gamble (2018) argues, society has to educate, empower and protect children and those who are working with them with the correct knowledge.

Early intervention for a younger age demographic is noted in the Internet Investigation Report (2020). For example, 95% of children who received online harm education in years 4-6 of primary school thought this was the right age. Nonetheless, as part of the UK government's mandatory Relationship, Health and Sex Education Programmes, primary school children are taught about the lesser dangers of online use.

Resultantly, primary school children are taught that 'sometimes people behave differently online; the rules and principles for keeping safe online and respect for others' and 'how to recognise harmful content and contact and report it'. Subsequently, rather than the risk of online sexual harm and engaging with strangers online, primary school children are taught to consider their online friendships and sources of information.

Yet, this guidance does not specify what 'keeping safe online' means. For example, younger children may not be taught in age-appropriate ways the risk of sharing self-generated content with others or using online games where children are sexually exploited for 'likes' and 'rewards'. According to the Department for Education (DOE) RSE Guidance Document (2022), primary schools are not obligated to teach sex education, however, as seen in Fig 6.1. DOE, RSE Guide (2022), the main responsibility for educating primary school children is excessive use, the negative aspects of the internet related to bullying and harassment and age restrictions on gaming sites and social media applications. No mention is made related to the online risks of sexual exploitation.

It is generally accepted that it is difficult to impose age restrictions on children and their social media and gaming use (Livingstone & Brake, 2010; Ybarra & Mitchell, 2008; Bernike & Anderson, 2023). Moreover, teaching children about age restrictions on social media apps will likely be ignored when children lie about their ages, presenting themselves as older (Herring & Kapidzic, 2015). Also, Hargittai et al. (2011) discuss the problems of parents helping children to lie about their ages to create social media accounts. As such, this thesis argues that there is a need for age-appropriate guidance and education for younger primary school children on social media use relating to sharing self-generated images and online games featuring rewards and likes.

Fig 6.1. The Department for Education (DOE) RSE Guidance Document (2022)

#### Internet Pupils should know safety and that for most people the internet is an integral part of life and has harms many benefits. about the benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing. how to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private. why social media, some computer games and online gaming, for example, are age restricted. that the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health. how to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted. where and how to report concerns and get support with issues online.

The online risk of much younger children is noted; however, it is prudent to ask if younger primary school-age children will fully understand the sensitive nature of online CSEM harms related to sharing images and potential exploitation by adults on specific gaming sites. In response, Barter et al. (2022) argue that younger children can understand sensitive issues such as online CSEM harms and contribute in a reliable and replicable manner. So, the evidence suggests that further studies should concentrate on developing age-appropriate educational interventions related to online harms involving gaming for much younger children and sharing self-generated images.

It has also been discussed that although girls aged 11-13 are at an elevated risk of online CSEM exploitation, boys are more at risk of the most severe category A image abuse, as evidenced by the IWF data. As also discussed, similar to younger children and their safeguarding interventions, practitioners and education staff should focus on age-appropriate education for boys relating to the risk of online exploitation and coercion regarding sharing images that involve penetrative abuse. Appropriately, more data relating to this issue needs to be gathered by way of quantitative and qualitative studies to indicate the full extent of this emerging problem.

When discussing the qualitative interview data, some findings of note have been explored. To remind the reader, some officers' online digital training and social media knowledge were inconsistent with what was expected of their role. Through various FOI requests, there appears to be an inconsistency in training among some police forces and officers working on online sexual crimes. Also, accreditation has been discussed for officers and staff working on online sexual crimes. Although each UK police force is operated independently, the author will argue that there is a need for formal consistency amongst all officers working in online CSEM investigations.

The concept of how police organisational leadership shares and retains knowledge of any changes in offending behaviour is another important factor noted in the discussion. In this study, interviewees claimed that online CSEM offenders are now engaging in all aspects of child sexual abuse offending behaviour and not specific genres. This theory contrasts in some ways with what is previously known about online CSEM offending behaviour related to the literature surrounding this issue. Still, as this study is only one exploration of a single police force, there is a strong argument for similar studies in other police forces nationwide. In that event, further research in this area will test the idea of 'complex offenders', or those who engage in all types of child sexual abuse and exploitation offending behaviour.

To conclude this chapter, this thesis has suggested that technology industries are now the primary responders to online CSEM countermeasures, with police playing a secondary role in arresting, interviewing and charging suspects. On this account, the technology industries must be kept updated by policing organisations on any new offending behaviours and use of technology by offenders to enable them to work collectively with criminal justice agencies to develop new and effective online technological countermeasures. However, this idea calls for government support with a national approach to collaborative working practices between policing organisations, charities invested in safeguarding children and the online technology industries.

'Police practices should be based on scientific evidence about what works best'
(Sherman, 1982, p.2)

### Chapter 7. The Conclusion

#### 7.1. The achievements of the study

This closing chapter highlights the achievements of this study which has identified vital issues which could lead to significant improvements in police practices related to online CSEM investigations. However, before addressing these issues, it is important to revisit the overarching research questions which ask, Are police officers keeping pace with technology-driven changes in online child sexual exploitation offending? This question underpins the whole emphasis of this study, to discover what is known about the training and knowledge of police officers and staff working in online sexual crimes investigation. As a former police detective who has previously worked in this online CSEM investigation, the author of this thesis wished to discover if the standard of training and knowledge had improved or changed from when they last worked in this environment in 2015.

In addressing the primary research question, it is also essential to remind the reader of the title of this thesis, namely, 'Exploring the police response to technology-driven changes in online child sexual exploitation offending.' Overall, the research questions cannot be properly addressed without first examining how policing organisations react to the fluid and changing nature of online technology used in CSEM offending. For example, this thesis explores the online digital knowledge and training of police officers working in frontline CSEM investigations and how this may impact future working practices. To this end, without first highlighting these issues it is difficult for policing and other organisations to adopt policy changes and working practice improvements in safeguarding children from online harm. To begin, there now follows a summary of the achievements highlighted in this work which are related to the specific research question.

#### 7.2. Police knowledge and training

This section is devoted to the main contributions and achievements identified within the study related to the participant interviews. If we begin by revisiting the primary research question, are police keeping pace with technological-driven changes in online CSEM offending', several concepts are explored and examined within this thesis. First, police officers in this study face several issues related to their knowledge and training concerning online technologies used in CSEM offending. Notably, the findings from the literature review shed light on police training related to cybercrime investigation; however, as previously discussed, most of the academic literature is focused on offences such as theft, fraud, and harassment rather than online CSEM investigations. Moreover, Sloan & Paoline (2021) posit that studies in police training usually relate to traditional training methods with recommendations for changes and evaluation. Ergo, it is appropriate that this study explores the training and knowledge of officers and staff working in online child sexual exploitation offending.

The participant interviews in this thesis add further weight to this debate by hearing the lived experiences of the officers and staff and their level of training, knowledge and understanding of online technology and social media platforms related to online CSEM offending. Notably, several issues have been highlighted which deserve specific attention related to future recommendations not only within policing but also within industry, education and society. To begin, the concept of official accreditation for officers working in online CSEM investigation is discussed.

#### 7.3. Official accreditation for officers

During the participant interviews, the subject of official accreditation for officers working in online CSEM investigation was raised. This issue is important as this thesis has illustrated that official accreditation for police officers usually involves those working in financial crime investigation units. Moreover, Hughes & Teodoro (2013) argue that police accreditation allows for diffusion and best practice which improves organisational performance and professionalism. Yet, given the serious nature of their roles and responsibilities, it is appropriate to question why police officers and civilian investigators in this area of work are not officially accredited in this role.

Regarding police officers training in online CSEM investigations, some forces in England and Wales insist that their officers are trained in all aspects of child sexual abuse inquiries by completing the specialist Child Abuse Investigation Development Course (SCAIDP) in addition to holding detective status and image grading training. Still, it is illustrated in this study that the SCAIDP course may not be useful for all police officers working in online sexual crimes investigation as the primary focus of this qualification is related to physical child sexual abuse.

The cost of the SCAIDP course is £750 per officer which argues that police leadership may be reluctant to invest this amount in a larger number of officers who were not specifically working in child abuse investigations. On the other hand, the SCAIDP course allows officers to work in all aspects of child sexual abuse investigations and equips them with the knowledge and skills to engage in all types of child abuse investigations. Additionally, officers who hold this qualification are accredited as PIP, Level 2, child abuse investigators, whereas officers working in online sexual crimes units without this are not. This being the case, this thesis gives prominence to the debate on professional accreditation and highlights the inequality of training and regulation for officers working in this area.

### 7.4. The level of social media knowledge and awareness of police officers and staff

A further issue illustrated within this study related to the social media knowledge and awareness of the participants related to their role in online CSEM investigation. When further exploring the technical and online digital awareness of officers working in online CSEM investigation, it would be expected that these officers had a certain degree of knowledge and awareness in these areas. However, It is during the participant interviews that we first come across the terms' Luddites' and 'technophobes' used by some participants to describe their colleague's understanding of online technology. Moreover, these phrases are not what one would expect when describing the knowledge of police officers and staff working in technology-enabled crime.

The inconsistencies between participants in their social media knowledge and awareness are further evident when police suspect interviews are discussed by the interviewees. Illustrating these issues, this thesis suggests that a lack of knowledge related to social media and other digital platforms used in CSEM offending may have implications for testing the truthfulness of suspects during the evidence-gathering process during police suspect interviews. However, evidence from this thesis suggests that if police officers do not understand how a social media application works, how do they know if a suspect is telling the truth? Consequently, the participant interviews highlight these issues, strengthening the argument that online digital and social media knowledge in online CSEM investigators should be mandatory and a formal part of self-directed learning and continuing professional development.

### 7.5. Retaining and sharing new knowledge of offending behaviours

Retaining knowledge concerning online offending behaviour was another essential factor within this thesis. It was evident during the participant interviews that officers and staff had observed new and significant changes in online CSEM offending behaviours. Yet despite noting these significant changes in online offending behaviours, this knowledge was not being retained or shared by senior police leadership with other police forces or academics.

Moreover, officers noted increases in sexualised chat referrals yet there was no evidence as to why and how there was a significant increase in this type of offence. Resultantly, this thesis will claim that without a formal process of retaining and sharing this knowledge, any important changes noted by officers in offending behaviour may be overlooked not only by the policing service but also by academics and scholars.

In response to this concern, a significant factor in this thesis suggests that online CSEM offenders are now offending across several spectrums of child sexual abuse. Indeed, this claim appears to contradict what is currently known about online CSEM offending behaviour. For example, the literature suggests that most online CSEM offenders do not usually cross over into physical or contact offending; however, the participant's working experience, suggests that this is now not the case.

To support this argument, recent work by Nicol et al. (2021) poses the question of whether individuals who access CSEM material are also physical contact offenders who use new technology or are a new type of child sex offender. In response to this question, this thesis suggests that in this study at least, online CSEM offenders are offending across several aspects of child sexual offending behaviour, including online grooming, possession and sharing of indecent images, sexualised chat with children, peer-to-peer sexualised chat and physical contact sexual abuse offending.

A primary aspect of this study involves the suggestion of 'complex offenders', which the author of this thesis has adapted from Krone's (2004) typology of offenders, which updates and takes into account how CSEM offenders are now using newer technolgy to offend such as online video platforms and deep-fake technolgy. As previously mentioned in this thesis, Krone (2004) typifies certain types of online offenders which include collectors, browsers, groomers, physical abusers, producers and distributors. However, whilst some of these typologies still exist over 20 years later, it is prudent to recognise the changes in the use of technolgy and offending behaviours of individuals who engage in child sexual abuse including online CSEM offending.

The suggestion that online CSEM offenders are now offending across several areas of child sexual offending behaviour may challenge our previous knowledge related to child sexual offending behaviour, however, identifying significant changes in CSEM offending behaviours is an important factor for policing organisations and how they respond to this issue by way of improvements to knowledge and training. Consequently, the idea of CSEM offenders now offending across several spectrums of child sexual abuse remains an important concern and one which must be addressed by way of further research. With this in mind, this thesis illustrates that recognising the significant changes in CSEM offending behaviour is crucial for practitioners and academics to improve service delivery, safeguard children and add to our academic knowledge.

### 7.6. Collaborative working experience

The issues of collaborative training of police officers working in CSEM investigations with other organisations, including the National Crime Agency, were also discussed in this thesis in the participant interviews. While not related to police training per se, it was nonetheless a relevant subject due to the impact on experience and learning.

For example, in the participant interviews, opinions were divided when the interviewees were asked about their ideas regarding work experience with the National Crime Agency (NCA). While some participants thought that work experience with the NCA was a good idea for gaining further knowledge, others were less enthusiastic, citing reasons such as the differences in policing and working in a non-police environment. This is an important factor as the online sexual crimes unit in this study works in collaboration with the NCA and receives regular crime referrals from them. Additionally, there appear to be some barriers regarding collaborative working as NCA staff may be from different non-policing civil service backgrounds, such as HMRC rather than criminal investigators. Accordingly, the barriers to collaborative working are noted by interviewees when they discuss the professional differences and rivalries between police officers and non-police organisations.

Yet despite the barriers identified to collaborative working practices, the work in this thesis strengthens the argument for supporting collaborative working in CSEM investigations teams by suggesting that police alone are ill-equipped to tackle the growing problem of online CSEM offending. At the same time, multi-disciplinary teams within child abuse investigation are not a novel approach, with some police forces across the UK adopting this idea. For example, stand-alone online CSEM teams, as noted in this thesis, could benefit from this approach. This being the case, this thesis highlights the benefits of collaborative working in online CSEM investigation teams, which should be encouraged by senior leadership to provide staff with the necessary skills, confidence and training.

### 7.7. How can police be better trained to investigate online CSEM?

Turning now to this underlying question, some responses are noted. To revisit the participant's narratives, the interviewee's opinions on this issue differed. Some participants described the training as 'ad-hock' and 'lacking.' At the same time, another interviewee claimed that further training was unnecessary as police detectives are primarily investigators, which is crucial to their role. Yet, despite these claims, all of the participants in this study appeared to accept that image grading training and having detective status were the principal qualifications for carrying out their roles.

Even so, this thesis has raised important issues in future training needs for officers working in online CSEM investigations. For example, self-directed learning and continuing personal development are essential factors for any professional organisation working in sensitive areas such as child abuse enquiries. Indeed, this was noted when participants claimed that the vast array of social media applications being introduced frequently prevented them from keeping up to date with the latest variants. Despite these claims, this thesis illustrates the importance of self-directed learning and CPD which can enhance professional knowledge and increase confidence among staff.

## 7.8. Official accreditation for officers working in online CSEM investigation

Despite officers holding detective status and in some cases image grading training, this thesis recommends that all officers and staff who work in the remit of online sexual crime investigation hold official accreditation appropriate to the serious and difficult nature of their role. Similar to financial investigators and PIP Level 2 child abuse investigators, an official accreditation not only singles out the officer's skills and expertise in the area of online CSEM investigation but also instils confidence within their role.

#### 7.9. Formal structures for learning and training

This thesis has demonstrated that in this study at least, there are no formal structures for officers training in this role other than learning from one another or learning 'as they go along'. Moreover, knowledge and training amongst staff related to online digital knowledge and social media are inconsistent, given the complex nature of their role. Suitably, the overall recommendation for policymakers is to address these factors. It was noted that officers did attend various courses on victimology, however, there was no formal or recognised training related to the use of online technology in online CSEM offending or the digital platforms used. Accordingly, senior leadership should encourage or have in place specific training and knowledge in this area by way of self-directed learning and continuing personal development.

### 7.10. Image grading training

Image grading was part of the requirement for officers and staff in this study to enable them to work in online sexual crime investigations. Yet, this thesis has highlighted issues in this process which suggests that image grading training is a subjective process. Indeed, this thesis suggests that Category C images are often used as a gauge to measure the severity of an offence rather than classified as an indecent image. Additionally, this study will also claim that category C images in the police force in this study were seen as a less serious offence by some senior leaders and prosecutors but not by the participants themselves who all agreed that class C images were indecent, and the classifications were merely sentencing tools.

In this respect, the evidence suggests that there is a need for policymakers and senior police leadership to treat all indecent image offences as a singular concern rather than a tool for triaging and investigative urgency.

#### 7.11. Retaining and sharing knowledge of new offending behaviours

This thesis has raised further issues related to sharing and knowledge retention when identifying new patterns of CSEM offending behaviours. For example, interviewees in this study have suggested that online CSEM offenders are now offending across all patterns of behaviours including sexual grooming, possession of indecent images, physical sexual abuse and sexualised chat with children, yet this knowledge was not being shared or retained within police the organisation or with academia. Resultantly, this thesis argues that senior police leadership should implement approved and tested learning theories where knowledge and new offending behaviours or offending intelligence can be retained and shared within the policing organisation. Consequently, this knowledge if suitably stored and retained can be used by scholars and academics for future research purposes.

After acknowledging the achievements identified in this study related to police training and knowledge, a natural progression, therefore, focuses on further issues identified within this study regarding the changes in online technology and CSEM offending and the role of the technology companies in the detection and removal of online CSEM.

# 7.12. Has the evolving nature of online digital technology changed offending behaviours?

This section of the thesis draws attention to live-stream CSEM offending and the risks to children. Previously in the discussion chapter of this work, the developmental changes in technology use such as live video platforms including Skype and Microsoft Teams suggest that especially in the COVID-19 era, this phenomenon has affected how children use online technology and the increased risk associated with this. Previously, the literature as illustrated in this thesis has focused on live-streaming abuse in South Asian areas across the globe. However, evidence in this thesis from the IWF data now suggests that more children from Western backgrounds are being sexually abused online via live-stream videos and are initially coerced on social media platforms.

This thesis claims that online technology has evolved and adapted so that online CSEM offenders can use sophisticated and improved technology to conduct their offending behaviour with minimal disruption. Drejer et al. (2024) highlight this concern by suggesting that social media and other digital platforms can live-stream video calls with ease. Moreover, Drejer et al. (2024) also posit that originally web cameras on larger devices such as laptops and stand-alone units were used for live streaming, however, with the fast-moving development in technology, live streaming can be used on almost any handheld or portable device including tablets and smartphones. Resultantly, the development of this technology has been used for nefarious purposes by online CSEM offenders.

Additionally, this thesis will claim that children who are sexually groomed on social media platforms are then directed by offenders to video messaging services to continue with live-stream abuse which may not be detectable by criminal justice agencies unless recorded. This is an important development in CSEM offending behaviour as previously, social media platforms such as Instagram and Facebook did not have the video messaging services which we now take for granted with each social media application. Therefore, this thesis suggests that online CSEM offenders have adapted to new changes in technology which have altered their offending behaviours.

# 7.13. Have the advances in online technology changed the risk to younger children?

Attention is now devoted to the analysis of the secondary data in Chapter 5 from the IWF and other sources which focuses on the increased risk to younger children from online CSEM offending. To begin, Chapter 2 the literature review supports the current data from the IWF which suggests that female children aged 11-13 are identified most in CSEM material and were also most at risk from sharing self-produced images. However, the data from the IWF now suggest that much younger children, under the age of 10 are now engaging in this high-risk online behaviour such as sharing self-generated images. Additionally, evidence from the participant interviews in this thesis suggests that much younger children are using YouTube to create videos sharing self-produced content.

However, it should be noted that this data is not representative of all police forces. Accordingly, these changes in online technology and behaviour have implications for children, especially those under 10 who are being placed at an increased risk and also challenge the current responses from criminal justice agencies and technology industries.

Further concerns are also noted in this thesis which illustrates how much younger children than previously known are now at an increased risk of CSEM abuse due to the accessibility and popularity of live-stream messaging platforms such as Skype, Messenger Video and Zoom. In addition, where the risk of live-stream sexual abuse was once commonly targeted against children from South Asian countries, technological advances suggest this is no longer the case. Accordingly, evidence in this thesis from the IWF data highlights the risks related to children from 'affluent' Western backgrounds who are now at an increased risk from online live-stream CSEM abuse in contrast to the literature which suggests that children from South Asian countries are most at risk.

The next section will highlight the changing role of the online technology industries' responses to online CSEM offending. This subject is a crucial aspect of society's responses to the ever-growing problem of online CSEM offending where the police are no longer able to compete with changes to offending behaviour and new and emerging technologies without the collaboration and intervention of the technology industries.

## 7.14. What is the changing role of the technology industries in online CSEM detection and countermeasures?

This thesis suggests that the technology industries are the primary countermeasures and responders to online CSEM offending, with police taking a secondary role in arresting and interviewing suspects. From a societal perspective, these claims may appear controversial to some; however, the literature within this thesis strengthens this argument by demonstrating the significant contribution to society and criminal justice agencies of the CSEM prevention and detection technology developed, shared, and used by the technology industries (Pereira et al., 2020; Independent Inquiry into Child Sexual Abuse, 2020; Child Dignity Alliance, 2020).

Thus, the need for collaboration between criminal justice agencies and the technology industries is evident within the context of this thesis which suggests that online CSEM technology is evolving beyond the capabilities of policing responses alone. To support this argument, the literature contained within this work claims that there are several reasons why police organisations are taking a secondary role in online CSEM investigations related to a lack of resources when investigating CSEM offending and investigators' lack of technical knowledge.

As Faubert et al. (2021) claim, the internet is endless, and an increase in the number of police officers investigating online offences would not register with the public. This being the case, this thesis brings ideas forward which argue for increased accountability related to joint organisational approaches with policing organisations and technology companies related to online safeguarding. In this context, this thesis suggests that no matter how many police officers are employed in a particular police force, if they are not sufficiently trained and supported by the technology industries, they cannot address the increasing challenge alone regarding the scale, pace and volume of online CSEM offending.

Additionally, to implement improvements in online technology and countermeasures, this thesis has illuminated the problems related to organisations sharing suitable data in a singular global depository to improve AI and machine learning in recognising and detecting online CSEM. Thus, police training and knowledge related to online CSEM offending have many facets, resulting in a complex relationship between police organisations, the technology industries, and other organisations invested in the online protection of children.

#### 7.15. Future outlook and recommendations

This study has addressed several issues related to online child sexual abuse and exploitation. Given the evidence so far, this thesis calls for specific attention and recommendations in the following areas:

- Official Accreditation and standardised training for all officers and staff working in online CSEM investigation,
- Collaborative training with partner organisations,
- A standardised approach to image grading training,
- Learning theories to be adopted by senior police leadership along with CPD for officers and staff related to social media and online digital platforms used in online CSEM offending,
- Further academic studies related to much younger children sharing intimate and inappropriate images online,
- Age-appropriate education and guidance for younger children and the online risks.

This thesis presents clear arguments which recommend that police officers and staff working in online CSEM investigation should hold official accreditation and have standardised training related to the serious nature of their roles. Furthermore, all officers and staff working in online CSEM investigation should undertake the specialist child abuse investigators development course (SCAIDP) as a standard part of their training. Touching upon this, other recommendations including self-directed learning and continuing personal development are essential factors for any professional organisation working in sensitive areas such as child abuse enquiries. Indeed, this area of interest was noted when participants in this study claimed that the vast array of social media applications being introduced frequently prevented them from keeping up to date with the latest variants.

Despite these claims, this thesis illustrates the importance of self-directed learning and CPD which can enhance professional knowledge and increase confidence among staff. Consequently, the participant interviews highlight these issues, strengthening the argument that online digital and social media knowledge in online CSEM investigators should be mandatory and a formal part of self-directed learning and continuing professional development.

Whilst self-directed learning is an important factor in police training, so too is the need for senior police leadership to understand and Implement the use of learning theories within their organisation to ensure that any knowledge of new and emerging offending behaviours is recorded and shared appropriately with other organisations and academics. Regarding image grading training, it is suggested within this thesis that this issue is a subjective process particularly when related to Category C images. Indeed, participants in this study highlighted issues such as the police organisation using categories as a triage method rather than its original purpose which is a charging and sentencing tool.

In this respect, this thesis recommends the need for policymakers and senior police leadership to treat all indecent image offences as a singular concern rather than as a tool for triaging and investigative urgency. Finally, collaborative training with partner organisations such as the NCA should be encouraged by senior police leadership to share good working practices and knowledge which will provide staff with the necessary skills and confidence needed to carry out their roles.

To finish this section, the evidence thus far calls for specific attention towards primary school-age children regarding appropriate guidance, educational resources and age-appropriate teaching of online safety for younger children regarding social media platforms and the safe use of live video platforms such as Messenger, Microsoft Teams, Zoom, Skype and Google Video. Despite the age limit of 13 on most social media platforms, evidence suggests that much younger children are using these digital platforms (Weeden et al., 2013).

Resultantly, this thesis suggests that younger children are using newer technology such as live video and live messaging platforms as a part of their everyday lives which have been appropriated by some individuals for illegal activity such as online CSEM offending. To this end, this thesis calls for age-appropriate online education risk prevention for children and safeguarding countermeasures for practitioners and digital platform service providers.

Finally, this thesis has highlighted the limitations and gaps within knowledge related to much younger children being placed at online risk from online games targeted at younger children for 'likes' and 'rewards'. This phenomenon is largely underrepresented by scholars and academics as much of the work in online games and risks to children usually relates to older teenage boys. In response to this concern, this thesis recommends further academic investigation in this area to add to our existing but limited knowledge on this subject.

#### 7.16. Feasibility and timeframe for recommendations

If we first look at the recommendations relating to formal accreditation, police training and knowledge it is useful to know that each of the police forces in England and Wales is accountable to local Police Crime Commissioners. As previously mentioned in this work, Crime Commissioners are 'to be the voice of the people and hold the police to account'. In addition, they are 'responsible for the totality of policing and to hold the Chief Constable to account' (The Association of Police Crime Commissioners, 2024). To this end, it should be noted that implementing changes as to how each specific police force conducts its training is limited by the governance of each Police Crime Commissioner.

In addition, it is well-reported that policing budgets are being scrutinised due to financial restrictions in budgeting which may present some difficulties, especially for smaller police forces. Illustrating this, The Police Federation of England (2022) argues that there has been no consideration by the UK Government given to investment in technology or services to enable the police to provide a high quality of policing which the public deserves. Resultantly, financial restraints may discourage some police forces from enrolling officers and staff on the SCAIDP course which costs an average of £750 per candidate. Given that policing in some roles is transitionary due to promotion to other departments and retirement, the cost of this course may not be a financially sound investment.

However, despite this limitation, this thesis has opened up a reasonable argument which calls for officers and staff to be trained in this area when working in all facets of child abuse investigations. For example, if officers are trained in all areas of child sexual abuse, and not solely online offending, policing units could be streamlined into a single unit which would be equipped to investigate all child sexual abuse investigations. One way of addressing this issue is to submit areas of interest of this thesis to The College of Policing.

The College of Policing is responsible in part for producing and sharing the latest research which identifies which policing activities work best through evidence-based policing (The College of Policing, 2024). Indeed, on its webpage, The College of Policing have a 'Practice Bank' where users can share good practices with organisations who are interested in crime reduction and criminal justice. According to The Colege of Policing, when sharing good work or practice, these interventions are not evaluated but include learning that can be shared. In addition, The College of Policing may require further information before any work is published. Resultantly, the author of this thesis feels that this intervention is an efficient and ideal method of sharing some parts of this study which may benefit the police service when addressing contentious issues such as online CSEM offending.

The author of this work is also conscious that in some aspects police organisations may be reluctant to allow researchers to conduct studies in some areas of the policing environment. This claim is illustrated in earlier work by Laycock (2001), who posits that researchers study police and tend to be critical of what they find because that is what researchers are trained to do. Resultantly, researchers should be prepared to accept that academic research within policing organisations can be a difficult process due to specific barriers such as trust. Despite the barriers experienced by the researcher in this study, it should be acknowledged that today, policing and criminal justice agencies are more open to research within their organisation.

In addition to The College of Policing, there are several respected academic journals related to policing such as The Police Journal, Theory, Practice and Principles. Moreover, The Police Journal is a peer-reviewed journal which provides a platform for academics and practitioners to collaborate and advance knowledge in different areas of policing through international dissemination. However, it should be noted that journal submissions are often not a quick process and may take some time to be accepted and published. Despite this, given that some participants in this study have identified changes in offending behaviours such as amendments to Krone's (2004) typology of offenders, this knowledge must be shared appropriately, not only within the academic community but also the police service as a whole. Therefore, submissions to academic journals will be considered where some of the ideas in this thesis may be shared with police organisations and the academic community to encourage the implementation of some of the recommendations in this work.

On a final point, it is also vital that the emerging trend identified in this thesis regarding much younger children, those under the age of 10 sharing intimate and inappropriate images should be appropriately addressed. In a similar vein, younger children being sexually exploited using online games is another area of concern. As the organisations who are invested in safeguarding children are vast, it is prudent to share aspects of this work with primary organisations such as the National Society for the Prevention of Cruelty to Children (NSCPP) and the Barnardo's Children's Charity. These organisations are well respected and work across many fields including educational establishments and informing parents and carers of new and emerging online risks to children. Subsequently, organisations such as this are an excellent conduit for sharing the emerging concerns illustrated in this thesis.

#### 7.17. Conclusion

To finish, the researcher suggests that the recommendations and concerns highlighted in this thesis may be beneficial to other researchers, academics and organisations, adding to our knowledge and understanding of online CSEM offending. Also, it would be beneficial for individual police forces to reflect on some of the recommendations made in this work by implementing the suggestions made which may improve the quality of service and increase public confidence.

Moreover, because of the work in this thesis, it is suggested that more attention is devoted

to the fundamental concerns of online CSEM offending, primarily safeguarding children

and their increased online risk. As online CSEM offending increases year on and technol-

ogy continues to adapt and evolve, policing organisations face an uphill battle to counter-

act this menace. As such, a whole societal approach is needed which will increase

knowledge and improve technological countermeasures regarding online protection and

the safeguarding of children.

The research and analysis in this thesis have provided excellent opportunities for aca-

demics, policymakers, technology industries and senior police leadership to consider

new approaches to tackling the global concern of online CSEM offending. From a policing

perspective, appropriate training and accreditation for officers and adopting learning

theories related to new offending behaviours are some ways in which police organisa-

tions can help achieve a standardised and effective response to online CSEM offending.

This study has also highlighted emerging concerns concerning online CSEM and its risks

to children from live video platforms, younger children sharing self-generated images,

social media and online games directed at younger children. Due to these concerns, po-

tential studies could emerge from this thesis focusing on the central issues highlighted.

Moreover, research and development in this area are crucial as online CSEM offending

behaviour is fluid and everchanging. In this manner, research's impact on society is cru-

cial in this context, as researchers and academics have an increased responsibility to ev-

idence the impact of their work in areas such as safeguarding and online harm protection.

Word count: 95,976

253

## References.

Abbas, N., & Policek, N. (2021). 'Don't be the same, be better: an exploratory study on police mobile technology resistance. *Police Practice and Research*, *22*(1), 849-868.

Abbott, O. (2023). Interactive universalism, the concrete other and discourse ethics: A sociological dialogue with Seyla Benhabib's theories of morality. *European Journal of Social Theory*, *26*(3), 335-353.

Açar, K. V. (2020). Framework for a single global repository of child abuse materials. *Global Policy*, *11*(1), 178-190.

Adjer, H., Patrini, G., Cavalli, F., & Cullen, L. (2019). Deeptrace, The State of Deepfakes, Landscapes, Threats and Impact. (Online). Retrieved on 13<sup>th</sup> March 2023 from <a href="https://docslib.org/doc/12559428/the-state-of-deepfakes-landscape">https://docslib.org/doc/12559428/the-state-of-deepfakes-landscape</a>.

Alazab, M. & Broadhurst, R. (2015). Spam and Criminal Activity (September 3, 2015). Trends and Issues in Crime And Criminal Justice (Australian Institute of Criminology) 2016, No 52 RegNet Research Paper No. 2014/44

Alderson P, Morrow V. 2004. Ethics, Social Research and Consulting with Children and Young People. Barnardo's: Ilford.

Alexy, E. M., Burgess, A.W, & Baker, T. (2005). Internet Offenders: Traders, travellers and combination travellers. *Journal of Interpersonal Violence*, 20,084-812.DOI: 01177/08862055276091

Allen, M. (2016). Police-reported crime statistics in Canada, 2015 (Report no 85-002-X) Ottawa, ON, Canada: Statistics Canada, Canadian Centre For Justice Statistics.

Alrwais, S., Liao, X., Mi, X., Wang, P., Wang, X., Qian, F., ... & McCoy, D. (2017, May). Under the shadow of sunshine: Understanding and detecting bulletproof hosting on legitimate service provider networks. In *2017 IEEE Symposium on Security and Privacy (SP)* (pp. 805-823). IEEE.

Alshamrani, S., Abusnaina, A., & Mohaisen, D. (2020, November). Hiding in plain sight: A measurement and analysis of kids' exposure to malicious URLs on YouTube. In *2020 IEEE/ACM Symposium on Edge Computing (SEC)* (pp. 321-326). IEEE.

Anderson, M., Faverio, M., Gottfried, J., (2022). Teens, Social Media and Technology. Pew Research Centre. (Online). Retrieved on 9<sup>th</sup> June 2023 from <a href="https://www.pewresearch.org/">https://www.pewresearch.org/</a>

Anderson, D.G. (2000). Coping strategies and burnout among veteran child protection workers, *Child Abuse & Neglect*, Vol. 24 No.6, pp.839-48

Andreescu, V. and Vito, G. (2010). 'An exploratory study on ideal leadership behaviour: The opinions of American police managers.' *International Journal of Police Science Management* 12(4): 567–583.

Andrews, L., Higgins, A., Andrews, M. W., & Lalor, J. G. (2012). Classic grounded theory to analyse secondary data: Reality and reflections. *Grounded Theory Review, 11*(1).

Annual Report (2017). World YWCA. (Online). Retrieved on 15<sup>th</sup> May 2023 from <a href="https://www.ywca.uk">https://www.ywca.uk</a>

Appel, M., Marker, C., & Gnambs, T. (2020). Are social media ruining our lives? A review of meta-analytic evidence. *Review of General Psychology*, *24*(1), 60-74.

Apple (2020). Apple Reports Record First Quarter Results. (Online) Accessed on 23rd March 2023 from: ://nr.apple.com/d2i8z883J5

Ariely, D., & Loewenstein, G. (2006). The heat of the moment: The effect of sexual arousal on sexual decision making. *Journal of behavioral decision making*, *19*(2), 87-98.

Armagh, D. S., Battaglia, N. L., & Lanning, K. V. (2000). Use of computers in the sexual exploitation of children (NCJ 170021). Washington, DC: U.S. Department of Justice (Online). Retrieved on 7<sup>th</sup> February 2022 from <a href="https://www.ojp.gov/ncjrs/virtual-library/abstracts/use-computers-sexual-exploitation-children">https://www.ojp.gov/ncjrs/virtual-library/abstracts/use-computers-sexual-exploitation-children</a>

Arnault, D. S., & Fetters, M. D. (2011). RO1 funding for mixed methods research: Lessons learned from the "Mixed-Method Analysis of Japanese Depression" project. *Journal of mixed methods research*, *5*(4), 309-329.

Ashurst, L., & McAlinden, A.-M. (2015). Young people, peer-to-peer grooming and sexual offending: Understanding and responding to harmful sexual behaviour within a social media society. *Probation Journal*, *62*(4), 374–388.

https://doi.org/10.1177/0264550515619572

Aslan, D. (2011). Critically evaluating typologies of internet sex offenders: A psychological perspective. *Journal of Forensic Psychology Practice*, *11*(5), 406-431.

Aslan. D & Edelmann. R (2014) Demographic and offence characteristics: a comparison of sex offenders convicted of possessing indecent images of children, committing contact sex offences or both offences. *The Journal of Forensic Psychiatry & Psychology Volume* 25, 2014 - Issue 2

Atkinson, P., Coffey, A., & Delamont, S. (2003). *Key themes in qualitative research: Continuities and changes.* Rowman Altamira.

Aurén, S., & Kuhlmann, D. F. (2015). Nipa Huts with High-Speed Internet: Commercial Exploitation of Children in the 21st Century. A Qualitative Investigation of Webcam Child Prostitution in the Philippines.

Autry, A. J., & Berge, Z. (2011). Digital natives and digital immigrants: getting to know each other. *Industrial and Commercial Training*, *43*(7), 460-466.

Ayling, J., & Grabosky, P. (2006). When police go shopping. *Policing: an international journal of police strategies & management*.

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

Babchishin, K.M, Meridan, H.L, Bartles, R.M, & Perkins, D. (2018). Child Sexual Exploitation Materials Offenders: A Review. *European Psychologist, (2018), Volume 23, Issue 1.* https://doi.org/10.1027/1016-9040/a000326

Babchishin. K, Hanson. K & VanZuylen. H (2014). Online Child pornography offenders are different: A Meta-analysis of the characteristics of online and offline sex offences against children. *Archives of Sexual Behaviour. Volume 44*, <u>Issue 1</u>, *pp 45–66* 

Bada, M., & Nurse, J. R. (2021, June). Profiling the cybercriminal: a systematic review of research. In *2021 international conference on cyber situational awareness, data analytics and assessment (CyberSA)* (pp. 1-8). IEEE.

Balfe, M., Gallagher, B., Masson, H., Balfe, S., Brugha, R., & Hackett, S. (2015). Internet child sex offenders' concerns about online security and their use of identity protection technologies: a review. *Child abuse review*, *24*(6), 427-439.

Barter, C., Batool, F., Charles, J., Devaney, J., Farrelly, N., Hayes, D., ... & Stanley, N. (2022). Conducting large-scale mixed-method research on harm and abuse prevention with children under 12: Learning from a UK feasibility study. *Children & Society*.

Bartov a', K., Androvicova, R., Krej ´cov ˇa, L., Weiss, P., & Klapilov ´a, K. (2021). The prevalence of 'paraphilic interests in the Czech population: Preference, arousal, the use of pornography, fantasy, and behaviour. *The Journal of Sex Research*, 58(1), 86–96. https://doi.org/10.1080/00224499.2019.170746

Basit, T. (2003). Manual or electronic? The role of coding in qualitative data analysis. *Educational research*, *45*(2), 143-154.

Bates, A., & Metcalf, C. (2007). A psychometric comparison of internet and non-internet sex offenders from a community treatment sample. *Journal of Sexual Aggression*, *13*(1), 11-20.

Bates, S. 2017. "Revenge Porn and Mental Health": A Qualitative Analysis of the Mental Health Effects of Revenge Porn on Female Survivors." *Feminist Criminology* 12 (1):22–42. doi: 10.1177/1557085116654565

Battelle, J. (2005). The birth of Google. Wired-san Francisco-, 13(8), 102.

Bazeley, P. (2004). Issues in mixing qualitative and quantitative approaches to research. *Applying qualitative methods to marketing management research*, *141*, 156.

BBC News, 20223, Ex-Met officer Police admits sending racist WhatsApp Messages. (Online). Retrieved on 6<sup>th</sup> November 2023 from <a href="https://www.bbc.co/news/uk-england-66743803">https://www.bbc.co/news/uk-england-66743803</a>

BBC (2021). Omegle: Children expose themselves on video chat sites. (Online). Retrieved on 20th Jan 2022, from https://www.bbc.co.uk/news/technology-56668156

BBC News (2017). Is your postman delivering drugs? (Online). Retrieved on 6<sup>th</sup> March 2023 from: https://www.bbc.co.uk/news/newsbeat-38223838

BBC News (2018). Can you become a detective in 12 weeks? (Online). Retrieved on 22<sup>nd</sup> February 2023 from https://www.bbc.co.uk/news/uk-44436292

BBC News (2020). UK's Internet use surges to a new high during lockdown. (Online). Retrieved on 10<sup>th</sup> April 2023 from: <a href="https://www.bbc.com/news/technology-53149268">https://www.bbc.com/news/technology-53149268</a>

BBC News (2022). Online Safety Bill. (Online). Retrieved on 9<sup>th</sup> February 2023 from <a href="https://www.bbc.co.uk/news/topics/c1llzgp5rvqt">https://www.bbc.co.uk/news/topics/c1llzgp5rvqt</a>

BBC News (2023). Lockdown Linked to Tenfold Rise in Child Abuse Imagery. (Online). Retrieved on 8<sup>th</sup> April 2023 from: <a href="https://www.bbc.co.uk/news/technology-64415015">https://www.bbc.co.uk/news/technology-64415015</a>

Bearman, M. (2019). Eliciting rich data: A practical approach to writing semi-structured interview schedules. *Focus on Health Professional Education: A Multi-Professional Journal*, *20*(3), 1-11.

Beaudry, A., & Pinsonneault, A. (2005). Understanding user responses to information technology: A coping model of user adaptation. *MIS Quarterly*, 493-524.

Becker, H.S. (1982). Culture. A Psychological View, Yale Review, 71:513-27

Becker, K., & Fitzpatrick, B. (2018). In search of shadows: investigating and prosecuting crime on the Dark Web. *Dep't of Just. J. Fed. L. & Prac.*, *66*, 41.

Beech, E., Birgden, A., Findlater, D. (2008). The Internet and Child Sexual Offending: A Criminological Review. *Aggression and Violent Behaviour* 13: 216-228

Beech. R, Elliot. A Mandeville- Norton. R & Hayes. E. (2009). Psychological Profiles of Internet Sexual Offenders: Comparisons with Contact Sexual Offenders. *Pub Med. Sexual Abuse. A Journal of Research and Treatment* 

Bell, L. & Allain, L. (2011) Exploring Professional Stereotypes and Learning for Inter-professional Practice: An Example from UK Qualifying Level Social Work Education, *Social Work Education*, 30:3, 266-80, DOI: 10.1080/02615479.2010.483726

Benhabib, S. (1994) 'In Defense of Universalism. Yet Again! A Response to Critics of Situating the Self', New German Critique, 62, pp.173–189.

Bennell, C., Alison, L. J., Stein, K. L., Alison, E. K., & Canter, D. V. (2001). Sexual offenses against children as the abusive exploitation of conventional adult-child relationships. *Journal of Social and Personal Relationships*, *18*(2), 155-171.

Bequai, A., & Crime, W. C. (1979). Fiedler, Judith (1978). Field Research: A Manual for Lo&tics and Management of Scientific Stud& in Natural.

Bernike, D., & Andersen, C. (2023). Presence of Age Restrictions for Children to Have Social Media Accounts in Law Number 27 of 2022 Concerning Personal Data Protection. *Riwayat: Educational Journal of History and Humanities, 6*(1).

Bhutta, Z. A. (2004). Beyond informed consent. *Bulletin of the World Health Organization*, 82, 771-777.

Bursztein, E., Clarke, E., DeLaune, M., Elifff, D. M., Hsu, N., Olson, L., ... & Bright, T. (2019, May). Rethinking the detection of child sexual abuse imagery on the internet. In *The world wide web conference* (pp. 2601-2607).

Biddle, P., England, P., Peinado, M, & Willman, B. (2002). The Darknet and the Future of Content Distribution. (Online). Retrieved on March 21, 2021, from <a href="https://www.cs.ucda-vis.edu/~rogaway/classes/188/spring06/darknet.pdf">https://www.cs.ucda-vis.edu/~rogaway/classes/188/spring06/darknet.pdf</a>

Birde, A. K., & Jain, M. (2020). *Organisational and Behavioural Work. Concepts and Analytical Approaches.* Apple Academic Press. Taylor and Francis.

Birimoglu Okuyan, C., & Begen, M. A. (2022). Working from home during the COVID-19 pandemic, its effects on health, and recommendations: The Pandemic and beyond. *Perspectives in Psychiatric Care*, *58*(1), 173-179.

Bloch-Wehba, H. (2021). Visible Policing: Technology, Transparency, and Democratic Control. *Cal. L. Rev.*, *109*, 917.

Bloom, S. (2014). No vengeance for revenge porn victims: Unraveling why this latest female-centric, intimate-partner offense is still legal, and why we should criminalize it. *Fordham Urb. LJ*, *42*, 233.

Blumer, H. (1962). Society as symbolic interaction. *Contemporary sociological thought*, 91.

Boaz, A., Hanney, S., Borst, R. *et al.* How to engage stakeholders in research: design principles to support improvement. *Health Res Policy Sys* **16**, 60 (2018).

https://doi.org/10.1186/s12961-018-0337-6

Boes, S., & Leukfeldt, E. R. (2016). Fighting cybercrime: joint effort. Ciber-Physical Security: Protecting Critical Infrastructure at the State and Local Level. Cincinnati.

Bogaerts, S., Vervaeke, G., & Goethals, J. (2004). A comparison of relational attitude and personality disorders in the explanation of child molestation. *Sexual Abuse: A Journal of Research and Treatment, 16*(1), 37-47.

Bogdan, R. and Biklen, S.K. (1992) *Qualitative Research for Education:* Boston, MA: Allyn & Bacon.

Bond, E. (2016). Sexting. *In Oxford research encyclopedia of criminology and criminal justice* 

Bond, E., & Tyrrell, K. (2021). Understanding revenge pornography: A national survey of police officers and staff in England and Wales. *Journal of interpersonal violence*, *36*(5-6), 2166-2181.

Boslaugh, S. (2007). *Secondary data sources for public health: A practical guide*. Cambridge University Press.

Bossler, A.M. and Holt, T.J. (2012), "Patrol officers' perceived role in responding to cybercrime", *Policing: An International Journal*, Vol. 35 No. 1, pp. 165-181. https://doi.org/10.1108/13639511211215504

Boulay, B., Coultas, J., & Luckin, R. (2008). How Compelling is the Evidence for the effectiveness of e-Learning in the Post-16 Sector? Brighton: University Sussex, *IDEAS Lab*.pp 1-145

Bourke, M. L., & Hernandez, A. E. (2009). The 'Butner Study'redux: A report of the incidence of hands-on child victimisation by child pornography offenders. *Journal of Family Violence*, *24*(3), 183-191.

Bourne, A. H., & Robson, M. A. (2015). Participants' reflections on being interviewed about risk and sexual behaviour: Implications for collection of qualitative data on sensitive topics. *International journal of social research methodology, 18*(1), 105-116.

Bradbury, D. (2014). Testing the defences of bulletproof hosting companies. *Network Security*, *2014*(6), 8-12.

Brady, P.Q. (2017). Crimes against caring: Exploring the risk of secondary traumatic stress, burnout and compassion satisfaction among child exploitation investigators. *Journal of Police and Criminal Psychology*, 32 (4), 305-318

Duggan, M., & Brenner, J. (2013). *The demographics of social media users, 2012* (Vol. 14). Washington, DC: Pew Research Center's Internet & American Life Project.

Bragias, A., Hine, K., & Fleet, R. (2021). 'Only in our best interest, right?' Public perceptions of police use of facial recognition technology. *Police Practice and Research*, *22*(6), 1637-1654.

Brannen, J. (1988). Research note the study of sensitive subjects. *The Sociological Review, 36*(3), 552-563.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3, 77-101.doi:10.1191/1478088706qp0630a.

Braun, V., & Clarke, V. (2014). Successful Qualitative Research. Sage Publications Ltd

Brennan M., Merdian H.L., Perkins D. (2017) Online Sex Offending and Risk Management. In: Kemshall H., McCartan K. (eds) *Contemporary Sex Offender Risk Management, Volume II. Palgrave Studies in Risk, Crime and Society. Palgrave Macmillan, Cham* 

Brennan, M., & Phippen, A. (2018). "Youth-Involved Sexual Imagery"—A Better Term to Challenge Blame Culture in Youth Sexting Cases?

Brenner, S.W. 2011. Defining cybercrime: A review of federal and state law. In Cybercrime: The investigation, prosecution, and defence of a computer-related crime, 3rd ed., ed. Clifford, Robert. D. 15–104. Raleigh, NC: Carolina Academic Press.

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

Brinkmann, S. & Kvale, S. *Doing Interviews* Vol. 2 (Sage, 2018)

British Psychological Society (2004). A Review of the Current Scientific Status and Fields of Application of Polygraph Deception Detection. Report (26/05/04) from the BPS Working Party.

Broadhurst, R. (2019). Child sex abuse images and exploitation materials. *Roderic Broadhurst, Child Sex Abuse Images and Exploitation Materials, in Roger Leukfeldt & Thomas Holt, Eds. Cybercrime: the human factor, Routledge.* 

Brodbeck, M. 1968. "*Meaning and Action*" in M. Brodbeck (ed.), Readings in the Philosophy of Social Science. New York: Macmillan

Brown, J. (1996), 'Police research: some critical issues', in F. Leishman, B. Loveday and S.P. Savage, Core Issues in Policing. London: Longman

Brown, J. (2020). Do graduate police officers make a difference to policing? Results of an integrative literature review. *Policing: A Journal of Policy and Practice, 14*(1), 9-30.

Bryce, J. (2010). Online sexual exploitation of children and young people. *Handbook of internet crime*, 320-342.

Bryman, A. (2010). Quantitative vs. qualitative methods. *Sociology: introductory readings, 47*.

Bryman, A. (2004). Qualitative research on leadership: A critical but appreciative review. *The leadership quarterly, 15*(6), 729-769.

Bryman, A. and Stephens, M. (1996). 'The importance of context: Qualitative research and the study of leadership.' *Leadership Quarterly* 7(3): 353–371.

Bryman, A., & Cramer, D. (2011). *Quantitative data analysis with IBM SPSS 17, 18 and 19*. Routledge.

Bullock, K. and Tilley, N. (2009). 'Evidence-Based Policing and Crime Reduction.' *Policing: A Journal of Policy and Practice*, 3(4): 381-387

Bullock, K., Sidebottom, A., Laycock, G., & Tilley, N. (2022). The diffusion of police innovation: A case study of problem-oriented policing in England and Wales. *International Journal of Police Science & Management*, *24*(4), 397-405.

Burawoy, M. (1982). *Manufacturing consent: Changes in the labor process under monopoly capitalism*. University of Chicago Press.

Burgess-Proctor, A., Patchin, J. W., & Hinduja, S. (2009). Cyberbullying and online harassment: Reconceptualizing the victimization of adolescent girls. *Female crime victims: Reality reconsidered*, *162*, 176.

Burnap, P., & Williams, M. L. (2016). Us and them: identifying cyber hate on Twitter across multiple protected characteristics. *EPJ Data science*, *5*, 1-15.

Burnett, M.E, Sheard, i., & St Clair-Thompson, H. (2020) The prevalence of compassion fatigue, compassion satisfaction and perceived stress, and their relationships with mental toughness, individual differences and number of self-care actions in a UK police force, *Police Practice and Research*, 21:4, 383-400, DOI: 10.1080/15614263.2019.1617144

Burruss, G, Howel, C.J, Bossler, A., & Holt, T.J. (2019) Self-perceptions of English and Welsh constables and sergeants preparedness for online crime: A latent class analysis, *Policing: An International Journal of Police Strategies and Management.* Vol. 43 No 1, pp. 105-119. DOI: 10.1108/PIJPSM-08-2019-0142

Bursztein, E., Clarke, E., DeLaune, M., Elifff, D. M., Hsu, N., Olson, L., ... & Bright, T. (2019, May). Rethinking the detection of child sexual abuse imagery on the internet. In *The world wide web conference* (pp. 2601-2607).

Bussy, K., & Grimbeek, E. J. (1995). Disclosure processes: Issues for child sexual abuse victims. In K. Rotenberg (Ed.), Disclosure processes in children and adolescents (pp. 166–203). New York: Cambridge University Press

Button, M., Frimpong, K., Smith, G., & Johnston, L. (2007). Professionalising counter fraud specialists in the U.K.: Assessing progress for reform. Crime Prevention and Community Safety, 9 (2)-101. Doi:http://dx.doi.org/10.1057/palrave.cpcs.8150037

Caless, B., & Owens, J. (2016). *Police and crime commissioners: The transformation of police accountability.* Policy Press.

Carr, N. (2020). The Shallows: *How the Internet Is Changing the Way We Think, Read and Remember.* Atlantic Books.

Ceccato, V. (2022). Fieldwork protocol as a safety inventory tool in public places. In *Field Studies in Environmental Criminology* (pp. 123-146). Routledge.

Cerf, V. G. (2008). The scope of Internet governance. In *Internet governance forum (IGF): The first two years* (pp. 51-56).

Chang, V. (2020). Tablet sales boosted by Covid-19 pandemic lockdown measures. (Online). Retrieved on 10<sup>th</sup> April 2023 from: <a href="https://www.straitstimes.com/tech/tablet">https://www.straitstimes.com/tech/tablet</a>.

Chau, P. Y., & Hu, P. J. (2002). Examining a model of information technology acceptance by individual professionals: An exploratory study. *Journal of management information systems*, *18*(4), 191-229.

Chave, D. (2017). Proceeds of crime training: Bringing it up to date. *Journal of Financial Crime*, *24*(3), 437-448. doi:http://dx.doi.org/10.1108/JFC-04-2017-0028

Chen, C. D. (1990). Computer crime and the computer fraud and abuse act of 1986. *Computer/L.J.*, *10*, 71.

Chih-Pei, H. U., & Chang, Y. Y. (2017). John W. Creswell, research design: Qualitative, quantitative, and mixed methods approaches. *Journal of Social and Administrative Sciences*, *4*(2), 205-207.

Child Dignity Alliance (2018). Technical Working Group Report. (Online). Retrieved on 1st October 2022 from <a href="https://www.childdignity.com/technical-working-group-report">https://www.childdignity.com/technical-working-group-report</a>

Choo, K. K. R. (2009). Online child grooming: A literature review on the misuse of social networking sites for grooming children for sexual offences.

Christner, N., Essler, S., Hazzam, A., & Paulus, M. (2021). Children's psychological well-being and problem behavior during the COVID-19 pandemic: An online study during the lockdown period in Germany. *PloS one*, *16*(6), e0253473.

Cole, R., Latif, S., & Chowdhury, M. M. (2021, October). Dark web: A facilitator of crime. In *2021 international conference on electrical, computer, communications and mechatronics engineering (iceccme)* (pp. 1-6). IEEE.

Chuang, S. (2021). The applications of constructivist learning theory and social learning theory on adult continuous development. *Performance Improvement*, *60*(3), 6-14.

Citron, D. K., & Franks, M. A. (2014). Criminalizing revenge porn. *Wake Forest L. Rev., 49*, 345.

Clancy, E. M., Klettke, B., Hallford, D. J., Crossman, A. M., Maas, M. K., & Toumbourou, J. W. (2020). Sharing is not always caring: Understanding motivations and behavioural associations with sext dissemination. *Computers in Human Behavior*, *112*, 106460.

Clark, T., Foster, L., Bryman, A., & Sloan, L. (2021). *Bryman's social research methods*. Oxford University Press.

Clark, V. L. P., & Ivankova, N. V. (2015). *Mixed methods research: A guide to the field* (Vol. 3). Sage publications.

Clarke, V., & Braun, V. (2013). Successful qualitative research: A practical guide for beginners. *Successful qualitative research*, 1-400.

Clennett-Sirois, L. (2014). It's Complicated: The Social Lives of Networked Teens. (Online). *The Canadian Journal of Communication*. Accessed on 2<sup>nd</sup> May 2023 from: <a href="https://doi.org/10.22230/cjc.2014v39n4a2917">https://doi.org/10.22230/cjc.2014v39n4a2917</a>

Cloudinary (2022). Understanding Image Hosting for Websites. (Online). Retrieved on 5<sup>th</sup> April 2023 from: <a href="https://cloudinary.com/.../understanding-image-hosting-for-websites">https://cloudinary.com/.../understanding-image-hosting-for-websites</a>

Cockcroft, t., Shan-A-Khuda, M., Schreuders, Z.C, & Trevorrow, P. (2020). Police Cybercrime Training: Perceptions, Pedagogy, and Policy, *Policing: A Journal of Policy and Practice*, Volume 15, Issue 1, March 2021, Pages 15–33, <a href="https://doi.org/10.1093/police/pay078">https://doi.org/10.1093/police/pay078</a>

Cohen-Almagore, R. (2013). Online Child Sex Offenders: Challenges and Countermeasures. *Howard Journal of Criminal Studies, Volume 52, Issue 2.* <a href="https://doi.org/10.1111/hojo.12006">https://doi.org/10.1111/hojo.12006</a>

College of Policing (2022) Investigative Interviewing. (Online). Retrieved on 7<sup>th</sup>

December 2022 from: <a href="https://www.college.police.uk/app/investigation/investigative-interviewing">https://www.college.police.uk/app/investigation/investigative-interviewing</a>

College of Policing (2022). Intelligence gathering. (Online). Retrieved on 26<sup>th</sup> September 2022 from <a href="https://www.college.police.uk/tags/intelligence-gathering">https://www.college.police.uk/tags/intelligence-gathering</a>

College of Policing (2022). Investigation Career Pathway. (Online). Retrieved on 10<sup>th</sup> May 2023 from: <a href="https://www.college.police.uk/career-learning/career-development">https://www.college.police.uk/career-learning/career-development</a>

College of Policing (2023) Child Abuse Investigator. (Online). Retrieved on 24<sup>th</sup> February 2023 from: https://profdev.college.police.uk/professional-profile/child-abuse-investigator

College of Policing. (2020). Supporting Effective Investigation: Help Shape our New Guidelines. (Online). Retrieved on February 16, 2021, from: <a href="https://www.college.police.uk/article/effective-investigations-guidelines-consultation">https://www.college.police.uk/article/effective-investigations-guidelines-consultation</a>

College of Policing: Briefing Note: Police Action in Response to Youth Produced Sexual Imagery (Sexting) (2016). <a href="https://www.westsussexscp.org.uk/wp-content/up-loads/Police-Action">https://www.westsussexscp.org.uk/wp-content/up-loads/Police-Action</a>.

Collins, E.C. (1992). Qualitative research as art: toward a holistic process. Theory into Pract. XXXI(2), 181–185

Conser, J. A. (1979). A literary review of the police subculture: Its characteristics, impact and policy implications. *Police Stud.: Int'l Rev. Police Dev.*, *2*, 46.

Cook, L. L., & Zschomler, D. (2020). Virtual home visits during the COVID-19 pandemic: Social workers' perspectives. *Practice*, *32*(5), 401-408.

Cooper, A. (1997). The Internet and sexuality: Into the next millennium. *Journal of Sex Education and Therapy*, *22*(1), 5-6.

Cooper, C., & Ingram, S. (2004). *Retention of police officers: a study of resignations and transfers in ten forces* (No. 86). London: Research, Development and Statistics Directorate, Home Office.

Cooper, K., Quayle, E., Jonsson, L., & Svedin, C. G. (2016). Adolescents and self-taken sexual images: A review of the literature. *Computers in human behavior*, *55*, 706-716.

Cooper. A. (1997) The Internet and Sexuality: Into the Next Millenium, *Journal of Sex Education and Therapy*, 22:1, 5-6, DOI: <u>10.1080/01614576.1997.11074164</u>

Cordner, C. (2020). *Police Sci. & Res. Bull. 53 (2020)* A Practical Approach to Evidence-Based Policing. (Online). Accessed on 19 August 2021 from https://heinonline.org/holcgi-bin/get\_pdf.cgi?handle=hein.journals/elerb20&section=9

Corti, L., Van den Eynden, V., Bishop, L., & Woollard, M. (2019). *Managing and sharing research data: A guide to good practice*. Sage.

Costinot, A., & Werning, I. (2018). *Robots, trade, and luddism: A sufficient statistic approach to optimal technology regulation* (No. w25103). National Bureau of Economic Research.

Cowburn, M. (2005). Confidentiality and public protection: ethical dilemmas in qualitative research with adult male sex offenders. *Journal of sexual aggression*, 11 (1), 49-63.

CPS (2017). Revenge Pornography Guidelines on prosecuting disclosing private sexual photographs or films. (Online ) Retrieved on 1st March 2023 from:

https://www.cps.gov.uk/legal-guidance/revenge-pornography-guidelines

Craven, S., Brown, S., & Gilchrist, E. (2006). Sexual grooming of children: Review of literature and theoretical considerations. *Journal of sexual aggression*, *12*(3), 287-299.

Creamer, E. G. (2018). Striving for methodological integrity in mixed methods research: The difference between mixed methods and mixed-up methods. *Journal of Engineering Education*, *107*(4), 526-530.

Creswell, W. (2014). Research design: Qualitative, quantitative and mixed methods approaches (4th ed.). Thousand Oaks, CA: Sage.

Creswell, J. W. (2014). *A concise introduction to mixed methods research*. SAGE publications.

Creswell, J. W., & Clark, V. L. P. (2017). *Designing and conducting mixed methods research*. Sage publications.

Creswell, J. W., & Poth, C. N. (2016). *Qualitative inquiry and research design: Choosing among five approaches.* Sage publications.

Creswell, J. W., Fetters, M. D., & Ivankova, N. V. (2004). Designing a mixed methods study in primary care. *The Annals of Family Medicine*, *2*(1), 7-12.

Creswell, JW, Plano Clark, VL (2007) Designing and Conducting Mixed Methods Research. Thousand Oaks, CA: Sage

Criddle, L. (2006). *Look Both Ways: Help protect your family on the Internet*. Washington, DC: Microsoft Press.

Crotty, M. J. (1998). The foundations of social research: Meaning and perspective in the research process. *The foundations of social research*, 1-256.

Cubitt, T. I., Napier, S., & Brown, R. (2023). Understanding the offline criminal behavior of individuals who live stream child sexual abuse. *Journal of interpersonal violence*, *38*(9-10), 6624-6649.

Cullen, O., Ernst, K. Z., Dawes, N., Binford, W., & Dimitropoulos, G. (2020). "Our laws have not caught up with the technology": Understanding challenges and facilitators in investigating and prosecuting child sexual abuse materials in the United States. *Laws*, *9*(4), 28.

Cummins Flory, T. A. (2016). Digital forensics in law enforcement: A needs-based analysis of Indiana agencies. *Journal of Digital Forensics, Security and Law, 11*(1), 4.

Cyber Tip Line Report (2021). National Centre for Missing Children. (Online) Retrieved on 28<sup>th</sup> October 2022 from: <a href="https://www.missingkids.org/gethelpnow/cyberti-pline/cybertiplinedata">https://www.missingkids.org/gethelpnow/cyberti-pline/cybertiplinedata</a>

Collier, B., Thomas, D. R., Clayton, R., Hutchings, A., & Chua, Y. T. (2022). Cybercrime is often hard to measure. Influence, infrastructure, and recentering cybercrime policing: Evaluating emerging approaches to online law enforcement through a market for cybercrime services. *Policing and Society, 32*(1), 103-124.

Dale, A., Arber, S., & Procter, M. (1988). *Doing secondary analysis*. Unwin Hyman.

Dalins, J., Tyshetskiy, Y., Wilson, C., Carman, M. J., & Boudry, D. (2018). Laying foundations for effective machine learning in law enforcement. Majura–A labelling schema for child exploitation materials. *Digital Investigation*, *26*, 40-54.

Dauvergne, M., & Turner, J. (2010). Police-reported crime statistics in Canada, 2009 (Report No. 85-002-X). Ottawa, ON Canada. Statistics Canada, Justice Canada.

Davidson, J., Schimmenti, A., Caretti, V., Puccia, A., Corbari, E., Bogaerts, S., ... & DeMarco, J. N. (2020). Exploring policing and industry practice in the prevention of online child sexual abuse. In *Child sexual abuse* (pp. 657-677). Academic Press.

DeMarco, J. N. (2020). Exploring policing and industry practice in the prevention of online child sexual abuse. In *Child sexual abuse* (pp. 657-677). Academic Press.

Davies, Pam, Rowe, Michael, Brown, D. M. and Biddle, Paul (2021) Understanding the status of evidence in policing research: reflections from a study of policing domestic abuse. *Policing and Society*, 31 (6). pp. 687-701. ISSN 1043-9463

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319-340.

Davis, G. (2020). Shining a Light on Policing of the Dark Web: An Analysis of U.K. Investigatory Powers. *The Journal of Criminal Law*, 2020, Vol. 84 (5) 407-426. DOI: 10.1177/0022018320952557

Davis, J.T. (2020). Computer Crime in North Carolina- Assessing the Needs Of Local Law Enforcement. GOVERNORS CRIME COMMISSION, North Carolina, US. Guba, E.G., Lincoln, Y.S., others, (1994). Competing Paradigms in qualitative research. *Handb. Qual. Res.* 2, 105

Davis, L., McShane, M. D., & Williams III, F. P. (1995). Controlling computer access to pornography: Special conditions for sex offenders. *Fed. Probation*, *59*, 43.

De Block, D., & Vis, B. (2019). Addressing the challenges related to transforming qualitative into quantitative data in qualitative comparative analysis. *Journal of Mixed Methods Research*, *13*(4), 503-535.

Decker, S. H. (2005). *Using offender interviews to inform police problem-solving*. US Department of Justice, Office of Community Oriented Policing Services.

Deloitte (2020). UK adults purchased up to 21 million new digital devices during lockdown. (Online). Retrieved on 10<sup>th</sup> April 2023 from:

https://www2.deloitte.com/uk/en/pages/press-releases/articles/uk.

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. *Networks and netwars: The future of terror, crime, and militancy, 239,* 288.

Denzin, N.K. and Lincoln, Y.S. (2018). *The SAGE handbook of qualitative research*. 5th ed, Los Angeles: SAGE.

Department of Education (2023). RSE Guidance Document. (Online). Retrieved on 25<sup>th</sup> May 2023 from: <a href="https://www.clareschool.co.uk/wp-content/uploads/2023/03/RSE-Policy-">https://www.clareschool.co.uk/wp-content/uploads/2023/03/RSE-Policy-</a>

DeVoe, E. R., & Faller, K. C. (2002). Questioning strategies in interviews with children who may have been sexually abused. *Child Welfare*, 81, 5–31.

Diefenbach, T. (2009). Are case studies more than sophisticated story telling? Methodological problems of case studies mainly based on semi-structured interviews. *Quality and Quantity, 43*(6), 875-894.

Diener, E., & Crandall, R. (1978). *Ethics in social and behavioral research*. U Chicago Press.

Dieronitou, I. (2014). The ontological and epistemological foundations of qualitative and quantitative approaches to research. *International Journal of Economics, Commerce and Management, 2*(10), 1-17.

Digital Evidence in U.K. Police Force (2020). *International Journal of Cyber Criminology-ISSN*: 0974-2891 January 2020. Vol 14(1): 316-340. DOI 10.5281/Zendo. 375721

Dockery, M., & Bawa, S. (2020). Working from Home in the COVID-19 Lockdown. *BCEC*, *19*, 1-5.

Dodge, A., Spencer, D., Ricciardelli, R., & Ballucci, D. (2019). "This isn't your father's police force": Digital evidence in sexual assault investigations. *Australian & New Zealand Journal of Criminology*, *52*(4), 499–515. https://doi.org/10.1177/0004865819851544.

Dodge, C., & Burrus, G. (2019). *Policing Cybercrime. The growing problem and considering future solutions. The Human Factor of Cybercrime.* Routledge. Electronic Crime Needs Assessment for State and Local Law Enforcement Series: *Research Report. NCJ.* 

Dokko, G., Wilk, S. L., & Rothbard, N. P. (2009). Unpacking prior experience: How career history affects job performance. *Organization Science*, *20*(1), 51-68.

Drejer, C., Riegler, M. A., Halvorsen, P., Johnson, M. S., & Baugerud, G. A. (2024). Livestreaming technology and online child sexual exploitation and abuse: A scoping review. *Trauma, violence, & abuse, 25*(1), 260-274.

Dul, J., & Hak, T. (2008). Case study methodology in business research. Abingdon, England: Routledge

Durkin, K. F. (1997). Misuse of the Internet by pedophiles: Implications for law enforcement and probation practice. *Fed. Probation, 61,* 14.

Durkin, K. F., & Bryant, C. D. (1995). "Log on to sex": Some notes on the carnal computer and erotic cyberspace as an emerging research frontier.

Durkin, K. F., & Bryant, C. D. (1999). Propagandizing pederasty: A thematic analysis of the online exculpatory accounts of unrepentant pedophiles. *Deviant Behavior*, *20*(2), 103-127.

Dushi, D. (2020). Combating the live-streaming of child sexual abuse and sexual exploitation: A need for new legislation. *Second international handbook of Internet research*, 201-223.

E. Rogers (1995). Diffusion of Innovations (4th ed) Free Press, New York (1995)

ECPAT International 2018. *Trends in online child sexual abuse material.* Bangkok: ECPAT International

Edwards, C., & Gribbon, L. (2013). Pathways to violent extremism in the digital era. *The RUSI Journal*, *158*(5), 40-47.

Egnoto, M., Ackerman, G., Iles, I., Roberts, H. A., Smith, D. S., Liu, B. F., & Behlendorf, B. (2017). What motivates the blue line for technology adoption? Insights from a police expert panel and survey. *Policing: An International Journal of Police Strategies & Management.* 

Eke, A. W., & Seto, M. C. (2022). Correspondence of child age and gender distribution in child sexual exploitation material and other child content with age and gender of child sexual assault victims. *Sexual Abuse*, 10790632221108951.

Ekström, M. (1992). Causal explanation of social action: the contribution of Max Weber and of critical realism to a generative view of causal explanation in social science. *Acta Sociologica*, *35*(2), 107-122.

Elliot, I.A, & Beech, A.R. (2009). Understanding online child pornography use: Applying sexual offence theory to internet offenders. *Aggression and Violent Behaviour*, Volume 14, Issue 3, Pages 180-193. <a href="https://doi.org/10.1016/j.avb.2009.03.002">https://doi.org/10.1016/j.avb.2009.03.002</a>

Elliot, I.A., Beech, A.R., & Manderville-Norden, R. (2013). The psychological profiles of Internet, contact and mixed Internet/contact sex offenders. *Sexual Abuse. A Journal of Research and Treatment*, 25, 3-20. doi:10.1177/1079063212439426

Elliott, E. & Vollm, B. (2016). *The Utility of Post-Conviction Polygraph Testing Amongst Sexual Offenders. The Division of Psychiatry and Applied Psychology, School of Medicine, The University of Nottingham.* 

Elmir, Rakime, Virginia Schmied, Debra Jackson, and Lesley Wilkes (2011). "Interviewing people about potentially sensitive topics." *Nurse Researcher* 19, no. 1 (2011).

Ennis, C. D., & Chen, S. (2012). Interviews and focus groups. In *Research methods in physical education and youth sport* (pp. 217-236). Routledge.

Eraker, E. C. (2010). Stemming sexting: Sensible legal approaches to teenagers' exchange of self-produced pornography. *Berkeley Tech. LJ, 25*, 555.

Escamilla, J. & Reichert, J., (2019). An Overview of Police Technology Adoption Efficacy. (Online). Retrieved on 2<sup>nd</sup> March 2022 from <a href="https://icjia.illinois.gov/researchhub/articles/an-overview-of-police-technology-adoption-and-efficacy">https://icjia.illinois.gov/researchhub/articles/an-overview-of-police-technology-adoption-and-efficacy</a>

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American journal of theoretical and applied statistics*, *5*(1), 1-4.

Euro News (2023). The EU tells Twitter to hire more human content moderators (Online). Retrieved on 9<sup>th</sup> March 2023 from:

 $\label{lem:https://cc.bingj.com/cache.aspx?q=Euro+News+(2023).+The+EU+tells+Twitter+to+hire+more+human+content+moderators+(Online).+Retrieved++on+9th+March+2023+from%3a+&d=4755757540591393&mkt=en-GB&setlang=en-GB&w=hagbhm8X8AVyq2FaHza6QWe092a2od0M$ 

European Commission (2020). Increased amount of child abuse material detected in Europe. (Online). Retrieved on 17<sup>th</sup> April 2023 from home-affairs.ec.europa.eu/news/increased-amount-child-sexual-abuse-material-

Europol (2015). Copyright European Financial Coalition against Commercial Sexual Exploitation of Children Online. EUROPOL. (Online). Retrieved on 27<sup>th</sup> April 2023 from: https://www.europol.europa.eu/cms/sites/default/files/documents/ef

Europol. (2017). *Internet Organised Crime Threat Assessment (IOCTA 2017)*. European Union Agency for Law Enforcement Cooperation (Europol).

Evang, A., & Øverlien, C. (2015). 'If you look, you have to leave': Young children regulating research interviews about experiences of domestic violence. *Journal of Early Childhood Research*, <u>13 (2)</u>, 113–125.10.1177/1476718X14538595

Evans, R., Pistrang, N., & Billings, J. (2013). Police officers' experiences of supportive and unsupportive social interactions following traumatic incidents. *European Journal of psychotraumatology*, *4*(1), 19696.

Fanniff, A. M., & Kimonis, E. R. (2014). Juveniles who have committed sexual offenses: A special group? *Behavioral sciences & the law, 32*(2), 240-257.

Farid, H. (2018). Reining in online abuses. *Technology & Innovation*, 19(3), 593-599.

Faubert, C., Décary-Hétu, D., Malm, A., Ratcliffe, J., & Dupont, B. (2021).

Law Enforcement and Disruption of Offline and Online Activities: A Review of Contemporary Challenges. *Cybercrime in Context: The human factor in victimisation, offending, and policing,* 351-370.

Fernandez, M., & Alani, H. (2021). Artificial intelligence and online extremism: Challenges and opportunities. *Predictive policing and artificial intelligence*, 132-162.

Fetters, M. D., Curry, L. A., & Creswell, J. W. (2013). Achieving integration in mixed methods designs—principles and practices. *Health services research*, *48*(6pt2), 2134-2156.

Feucht, F. (2017). The epistemic beliefs of fourth graders about the verification of second-hand knowledge and its knowledge sources. *Journal of Education and Human Development*, *6*(1), 7-26.

Figley, C.R. (1995), in Figley, C.R. (Ed). *Compassion Fatigue: Coping with Secondary Traumatic Stress Disorder in Those Who Treat Traumatised, Compassion Fatigue as Secondary Traumatic Stress Disorder: An Overview, Brunner-Routledge, New York, pp. 1-20.* 

Finkelhor, D. (1984). Child sexual abuse. *New Theory and Research*. Free press. *New York*, 186f.

Finkelhor, D., Hotaling, G., Lewis, I., & Smith, C. (1990). Sexual abuse in a national survey of adult men and women: Prevalence, characteristics, and risk factors. *Child Abuse & Neglect*, 14, 19–28

Finkelhor, D., Turner, H., & Colburn, D. (2022). Prevalence of online sexual offenses against children in the US. *JAMA network open*, *5*(10), e2234471-e2234471.

Finkelhor, D., Ormrod, R., & Chaffin, M. (2009). *Juveniles who commit sex offenses against minors. Juvenile Justice Bulletin*. Washington, DC: Office of Juvenile Justice and Delinquency Prevention.

Finlay, L. (2002). Negotiating the swamp: the opportunity and challenge of reflexivity in research practice. *Qualitative research*, *2*(2), 209-230.

Fleming, M. J., Greentree, S., Cocotti-Muller, D., Elias, K. A., & Morrison, S. (2006). Safety in cyberspace: Adolescents' safety and exposure online. *Youth & Society*, 38(2), 135–154. doi:10.1177/0044118X06287858

Flick, U. (2014) 5th Ed. An introduction to qualitative research. SAGE Publications: London

Flynn PM, Simpson DD. Adoption and implementation of evidence-based treatment. In: Miller PM, editor. *Evidence-based addiction treatment.* Elsevier; San Diego, CA: 2009. pp. 419–437

Follette, V. M., Polusny, M. M., & Milbeck, K. (1994). Mental health and law enforcement professionals: Trauma history, psychological symptoms, and impact of providing services to child sexual abuse survivors. *Professional psychology: Research and practice, 25*(3), 275.

Forbes (2023). TikTok moderators are being trained using graphic images of children being sexually exploited. (Online). Retrieved on 9th March 2023 from: https://www.forbes.com/sites/alexandralevine/2022/08/04/tiktok-is

Fortin, F., Paquette, P. & Dupont, B. (2018). From Online to Offline Sexual Offending. *Aggression and Violent Behaviour*, Pages 33-41

Fox, J., & Vendemia, M. A. (2016). Selective self-presentation and social comparison through photographs on social networking sites. *Cyberpsychology, Behavior, and Social Networking*, 19(10), 593–600. https://doi.org/10.1089/cyber.2016.0248

Fox, S. J. (2018). Positioning the Drone: Policing the Risky Skies. *Issues Aviation L. & Pol'y, 18,* 295.

Franklin, J., Perrig, A., Paxson, V., & Savage, S. (2007). An inquiry into the nature and causes of the wealth of internet miscreants. *Ccs*, *7*, 375-388.

Franqueira, V. N., Bryce, J., Al Mutawa, N., & Marrington, A. (2018). Investigation of Indecent Images of Children cases: Challenges and suggestions collected from the trenches. *Digital Investigation*, *24*, 95-105.

Franzosi, R. (2012). 'The difficulty of mixed-method approaches'. *Sociological Methodology*, 42(1), pp. 79-81.

Fromberger, P., Jordan, K., & Müller, J. L. (2018). Virtual reality applications for diagnosis, risk assessment and therapy of child abusers. Behavioral Sciences & the Law, 36(2), 235–244.

Furnell, S. (2002). *Cybercrime: Vandalizing the information society* (pp. 3-540). London: Addison-Wesley.

Furnell, S., & Dowling, S. (2019). Cybercrime: a portrait of the landscape. *Journal of Criminological Research, Policy and Practice, 5*(1), 13-26.

Gabriel, M. G., Brown, A., León, M., & Outley, C. (2020). Power and social control of youth during the COVID-19 pandemic. *Leisure Sciences*, 43(1–2), 1–7. https://doi.org/10.1080/01490400.2020.1774008

Gailloux, C., Furness, W. W., Myles, C. C., Wiley, D. S., & Collins, K. (2022). Fieldwork without the field: Navigating qualitative research in pandemic times. *Frontiers in Sustainable Food Systems*, *6*, 750409.

Gallagher, B. (2007). Internet –Initiated Incitement and Conspiracy to Commit Child Sexual Abuse (CSA): The Typology, Extent and Nature of Known cases. *Journal of Sexual Aggression* 13:101-119

Gallagher, M., Haywood, S. L., Jones, M. W., & Milne, S. (2010). Negotiating informed consent with children in school-based research: a critical review. *Children & society*, *24*(6), 471-482.

García Jiménez, A., & Montes Vozmediano, M. (2020). Subject matter of videos for teens on YouTube. *International Journal of adolescence and youth, 25*(1), 63-78.

Garlen, J. C., & Hembruff, S. L. (2021). Unboxing Childhood: Risk and Responsibility in the Age of YouTube. *Journal of Childhood Studies*, 78-90.

Garrison, D.R. & Cleveland-Innes, M. (2005) Facilitating Cognitive Presence in Online Learning: interaction is not enough, *American Journal of Distance Education*, 19(3), 133. <a href="http://dx.doi.org/10.1207/s15389286ajde1903\_2">http://dx.doi.org/10.1207/s15389286ajde1903\_2</a>

Gerstenfeld, P. B., Grant, D. R., & Chiang, C. P. (2003). Hate online: A content analysis of extremist Internet sites. *Analyses of social issues and public policy*, *3*(1), 29-44.

Galletta, A. (2013). *Mastering the semi-structured interview and beyond: From research design to analysis and publication* (Vol. 18). NYU Press.

Ghosh, R., Dubey, M. J., Chatterjee, S., & Dubey, S. (2020). Impact of COVID-19 on children: Special focus on the psychosocial aspect. *Minerva Pediatrica*, 72(3), 226–235. <a href="https://doi.org/10.23736/S0026-4946.20.05887-9">https://doi.org/10.23736/S0026-4946.20.05887-9</a>

Gieseke, A. P. (2020). "The New Weapon of Choice": Law's Current Inability to Properly Address Deepfake Pornography. *Vand. L. Rev., 73,* 1479.

Gillespie T (2020) Content moderation, AI, and the question of scale. *Big Data & Society* 7(2): 2053951720943234.

Gilmour, P. M. (2021). Exploring the barriers to policing financial crime in England and Wales. *Policing: A Journal of Policy and Practice*, *15*(2), 1507-1521.

Glaser, B. G. (1962). Secondary analysis: A strategy for the use of knowledge from research elsewhere. *Soc. Probs.*, *10*, 70.

Glasgow, D. (2010). The potential of digital evidence to contribute to risk assessment of internet offenders. *Journal of Sexual Aggression*, 16(1), 87–106.

https://doi.org/10.1080/13552600903428839

Glass, C. R. 2013. "Strengthening and Deepening Education for Personal and Social Responsibility." *New Directions for Higher Education* 2013: 83–94.10.1002/he.v2013.164

Glesne, C. (2015). *Becoming qualitative researchers: An introduction*. Pearson.

Global Overview Report (2022). (Online). Retrieved on 12<sup>th</sup> June 2023 from <a href="https://datareportal.com/reports/digital-2022-global-overview-report">https://datareportal.com/reports/digital-2022-global-overview-report</a>

Goertzen, M. J. (2017). Introduction to quantitative research and data. *Library Technology Reports*, *53*(4), 12-18.

Goodman, M. (2015). Future crimes: Inside the digital underground and the battle for our connected world. Random House.

Goodwill, A. M., Lehmann, R. J. B., Beauregard, E., & Andrei, A. (2016). An action phase approach to offender profiling. *Legal and Criminological Psychology*, 21(2), 229–250. https://doi.org/10.1111/lcrp.12069.

Gorden, S., & Ford, R (2003). Cyberterrorism? Cuopertino CA: Symantec.

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

Gov. UK (2023). Strategic Policing Requirement (2023). (Online). Retrieved on 12<sup>th</sup> May 2023 from: <a href="https://www.gov.uk/government/publications/strategic-policing-require-ment-2023">https://www.gov.uk/government/publications/strategic-policing-require-ment-2023</a>

Gov. UK. (2022). Police Workforce England and Wales.(Online) Retrieved on 24<sup>th</sup> May 2023 from <a href="https://www.gov.uk/government/statistics/police/workforce-england-and-wales">https://www.gov.uk/government/statistics/police/workforce-england-and-wales</a>

Graef, M.I, & Hill, EL (2000). Costing child protective services staff turnover, *Child welfare*, Vol. 79 No 5, pp. 517-33

Greenhalgh T, Robert G, Macfarlane F et al. (2004) Diffusion of innovations in service organizations: systematic review and recommendations. *Milbank Quarterly* 82(4): 581–629

Grieco, J., Vovak, H., & Lum, C. (2014). Examining research–practice partnerships in policing evaluations. *Policing: A Journal of Policy and Practice*, *8*(4), 368-378.

Gries, L. T., Goh, D. S., & Cavanaugh, J. (1996). Factors associated with disclosure during child sexual abuse assessment. *Journal of Child Sexual Abuse*, 5, 1–19.

Griffiths, M.D. (2012). Internet sex addiction: A review of empirical research. *Addiction Research & Theory, Volume, 20, Issue 2, Pages 111-124.* 

Grinnell Jr, R. M., & Unrau, Y. A. (2010). *Social work research and evaluation: Foundations of evidence-based practice*. Oxford University Press.

Gross, M. L., Canetti, D., & Vashdi, D. R. (2016). The psychological effects of cyber terrorism. *Bulletin of the Atomic Scientists*, *72*(5), 284-291.

Grosskopf, A. (2010). Online interactions involving suspected paedophiles who engage male children. *Trends and Issues in Crime and Criminal Justice*, (403), 1-6.

Grubin, D., Kamenskov, M., Dwyer, R. G., & Stephenson, T. (2019). Post-conviction polygraph testing of sex offenders. *International Review of Psychiatry*, *31*(2), 141-148. <a href="https://doi.org/10.1080/09540261.2018.1561428">https://doi.org/10.1080/09540261.2018.1561428</a>

Gruen, M. (2006). Innovative recruitment and indoctrination tactics by extremists: Video games, hip-hop, and the world wide web. *The making of a terrorist, 1*, 11-22.

Guba E. G., Lincoln Y. (1989). Fourth-generation evaluation. Newbury Park, CA: Sage.

Guba, E. and Lincoln, Y. (1985) Naturalistic Inquiry. Newbury Park, CA: Sage.

Guerra, E., & Westlake, B. G. (2021). Detecting child sexual abuse images: traits of child sexual exploitation hosting and displaying websites. *Child Abuse & Neglect*, *122*, 105336.

Guetterman, T. C., Fetters, M. D., & Creswell, J. W. (2015). Integrating quantitative and qualitative results in health science mixed methods research through joint displays. *The Annals of Family Medicine*, *13*(6), 554-561.

Guzzetta, Baldini, S., Bancale, A., Baroncelli, L., Ciucci, F., Ghirri, P., Putignano, E., Sale, A., Viegi, A., Berardi, N., Boldrini, A., Cioni, G., Maffei, L. (2009). Massage Accelerates Brain Development and the Maturation of Visual Function. *The Journal of Neuroscience* 29(18), 6042–6051

Hackett, S. (2014). *Children and young people with harmful sexual behaviours*. Dartington: Research in Practice.

Hadlington, L., Lumsden, K., Black, A., & Ferra, (2018). A Qualitative Exploration of Police Officers Experiences, Challenges and Perceptions of Policing Cybercrime. <a href="https://doi.org/10.1093/police/pay090">https://doi.org/10.1093/police/pay090</a>

Haig-Ferguson, A., Cooper, K., Cartwright, E., Loades, M. E., & Daniels, J. (2021). Practitioner review: Health anxiety in children and young people in the context of the COVID-19 pandemic. *Behavioural and cognitive psychotherapy*, *49*(2), 129-143.

Hamlyn, D. W. (1995). Epistemology, history of. *The Oxford companion to philosophy*, 242-245.

Hargittai, E., Schultz, J., & Palfrey, J. (2011). Why parents help their children lie to Face-book about age: Unintended consequences of the 'Children's Online Privacy Protection Act'. *First Monday* 

Harichandran, V.S., Breitinger, F., Baggali, I., & Marrington, A. (2016). A cyber forensics needs analysis survey: Revisiting the domain's needs a decade later. *Comput Secur*. 57, 1-13. DOI: 10.1016/j.cose. 2015.10.007

Harkin, D., Whelan, D, & Chang, L. (2018) The challenges facing specialist police cybercrime units: an empirical analysis, *Police Practice and Research*, 19:6, 519-536, DOI: 10.1080/15614263.2018.1507889

Harrison, H., Birks, M., Franklin, R., & Mills, J. (2017, January). Case study research: Foundations and methodological orientations. In *Forum qualitative Sozialforschung/Forum: qualitative social research* (Vol. 18, No. 1).

Hatta, T., Narita, K., Yanagihara, K., Ishiguro, H., Murayama, T., & Yokode, M. (2020). Crossover mixed analysis in a convergent mixed methods design used to investigate clinical dialogues about cancer treatment in the Japanese context. Journal of Mixed Methods Research, 14(1), 84–109. https://doi.org/10.1177/1558689818792793

Hattingh, M. (2021). The Dark Side of YouTube: A Systematic Review of Literature. *Adolescences*.

Hauben, M., & Hauben, R. (1998). The Net and Netizens: The Impact of the Net on People's Lives (Chapter 1). *First Monday*.

Heath S, Charles V, Crow G, Wiles R. 2007. Informed consent, gatekeepers and gobetweens: negotiating consent in child and youth-orientated institutions. *British Educational Research Journal* 33:403–417

Heaton, J. (2008). Secondary analysis of qualitative data: An overview. *Historical Social Research/Historische Sozialforschung*, 33-45.

Hekman, S. J. (1979). Weber's concept of causality and the modern critique. *Sociological Inquiry*, *49*(4), 67-76.

Henney, J. E., Shuren, J. E., Nightingale, S. L., & McGinnis, T. J. (1999). Internet purchase of prescription drugs: buyer beware. *Annals of internal medicine*, *131*(11), 861-862.

Henry, O., Mandeville-Norden, R., Hayes, E., & Egan, V. (2010). Do internet-based sexual offenders reduce to normal, inadequate and deviant groups? *Journal of Sexual Aggression*, *16*(1), 33-46.

Herbert, J. L., & Bromfield, L. (2019). Better together? A review of evidence for multi-disciplinary teams responding to physical and sexual child abuse. *Trauma, Violence, & Abuse, 20*(2), 214-228.

Herd, G. (2017). Minecraft: Grooming dangers for children gaming online. BBC News. (Online). Retrieved on May 3, 2023, from: <a href="https://www.bbc.com/news/uk-wales-38284216">https://www.bbc.com/news/uk-wales-38284216</a>

Hernandez, S. C. L. S., Lacsina, A. C., Ylade, M. C., Aldaba, J., Lam, H. Y., Estacio Jr, L. R., & Lopez, A. L. (2018). Sexual exploitation and abuse of children online in the Philippines: a review of online news and articles. *Acta Medica Philippina*, *52*(4).

Herring, S. C., & Kapidzic, S. (2015). Teens, gender, and self-presentation in social media. *International encyclopedia of social and behavioral sciences, 2,* 1-16.

Hershkowitz, I. (2006). Delayed disclosure of alleged child abuse victims in Israel. *The American Journal of Orthopsychiatry*, 76(4), 444–450. doi:10.1037/0002-9432.76.4.444

Herva, S. (1988). The genesis of Max Weber's verstehende soziologie. *Acta Sociologica*, *31*(2), 143-156.

Herzog, C., Handke, C., & Hitters, E. (2019). *Analyzing talk and text II: Thematic analysis* (pp. 385-401). Springer International Publishing.

Heslop, R. (2011). Community engagement and learning as 'becoming': Findings from a study of British police recruit training. *Policing and society, 21*(3), 327-342.

Hewitt, J. (2007). Ethical components of researcher—researched relationships in qualitative interviewing. *Qualitative health research*, *17*(8), 1149-1159.

Hicks, C. (1995). The shortfall in published research: a study of nurses' research and publication activities. *Journal of Advanced Nursing*, *21*(3), 594-604.

Hill, L. (2015). 'Don't make us talk!': Listening to and learning from children and young people living with parental alcohol problems. *Children & Society*, *29*, 344–354.10.1111/chso.2015.29.issue-5

Hill (2020). A Complete History of the Camera Phone, Digital Trends. (Online). Retrieved on March 23, 2023, from: <a href="https://www.digitaltrends.com/mobile/camera-phone-history">https://www.digitaltrends.com/mobile/camera-phone-history</a>

Hinduja, S. (2004). Perceptions of Local Law Enforcement Concerning the Role of and State Computer Crime Investigation Team. *Policing: An International Journal of Police Strategie & Management*, 27: 341-357.

Hirschheim, R., & Newman, M. (1988). Information systems and user resistance: theory and practice. *The Computer Journal*, *31*(5), 398-408.

HMIC, 2017. State of Policing: The annual assessment of policing in England and Wales, 2016. (Online). Retrieved on 7<sup>th</sup> September 2022 from:

https://www.justiceinspectorates.gov.uk/hmic/wp-content/uploads/state-of-policing-2016.pdf

Hogan, M., & Strasburger, V. C. (2018). Social media and new technology: A primer. *Clinical Pediatrics*, *57*(10), 1204-1215.

Holdaway, S. (1982). An Inside Job in Bulmer, M. Social Research Ethics.

Holt, T. J. (2012). Exploring the intersections of technology, crime and terror. *Terrorism and Political Violence*, 24, 337–354.

Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets online: products and market forces. *Criminal Justice Studies*, *23*(1), 33-50.

Holt, T. J., Blevins, K. R., & Burkert, N. (2010). Considering the pedophile subculture online. *Sexual Abuse*, *22*(1), 3-24.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2017). *Cybercrime and digital forensics: 3<sup>RD</sup> Ed, An introduction*. Routledge.

Holt, T. J., Burruss, G., & Bossler, A. (2015). Policing cybercrime and cyberterror.

Holt, T., & Bossler, A. (2015). *Cybercrime in progress: Theory and prevention of technol-ogy-enabled offenses.* Routledge.

Holt, T., Freilich, J. D., Chermak, S., & McCauley, C. (2015). Political radicalization on the Internet: Extremist content, government control, and the power of victim and jihad videos. *Dynamics of Asymmetric Conflict*, 8(2), 107-120.

Holt, T., Kristie, B., & Burker, N. (2010). Considering the Pedophile Subculture Online. *Sexual Abuse* 22:3-24

Home Office Child Database (2018). (Online). Accessed on 21st January 2022 fromhttps://www.digitalmarketplace.service.gov.uk/g-cloud/services/293090742561273

Honess, R. (2020). Mandatory police training: the epitome of dissatisfaction and demotivation? *Policing: A Journal of Policy and Practice*, *14*(1), 191-201.

Honts, C.R., & Reavy, R. (2015). *The comparison question polygraph test: A contrast of methods and scoring. Physiology and Behaviour, 143, 15-26* 

House of Commons Science and Technology Committee Impact of social media and screen-use on young people's health (2019). (Online). Retrieved on March 20, 2021, from <a href="https://publications.parlia-">https://publications.parlia-</a>

ment.uk/pa/cm201719/cmselect/cmsctech/822/822.pdf#:~:text=Pub-lished%20on%2031%20January%202019%20by%20authority%20of,Government%200ffice%20for%20Science%20and%20associated%20public%20bodies.

Houtepen, J., Sijsema. J.J., & Bogaerts, S. (2014). From child pornography offending to child sexual abuse: A review of child pornography offender characteristics and risk of cross-over. *Aggression and Violent Behaviour*, Volume 19, Issue 5. https://doi.org/10.1016/j.avb.2014.07.011

Howell, K. E. (2012). An introduction to the philosophy of methodology. Sage.

Howes, L. M., & Goodman-Delahunty, J. (2015). Career decisions by Australian police officers: a cross-section of perspectives on entering, staying in and leaving policing careers. *Police practice and research*, *16*(6), 453-468.

Howitt, D., & Sheldon, K. (2007). The role of cognitive distortions in paedophilic offending: Internet and contact offenders compared. Psychology, *Crime & Law*, 13, 469-486. DOI: 10.1080/10683160601060564

Hruska, J., & Maresova, P. (2020). Use of social media platforms among adults in the United States—behavior on social media. *Societies*, *10*(1), 27.

Huang, J. H., Lin, Y. R., & Chuang, S. T. (2007). Elucidating user behavior of mobile learning: A perspective of the extended technology acceptance model. *The electronic library*.

Hug, B, & McNeill, K.L. (2008) Use of First-hand and Second-hand Data in Science: Does data type influence classroom conversations? *International Journal of Science Education, 30:13,* 1725-1751, DOI: 10.1080/0950069070150694

Hughes, A. G., & Teodoro, M. P. (2013). Assessing professionalism: Street-level attitudes and agency accreditation. *State and Local Government Review, 45*(1), 36-45.

Hughes, B., Parker, H., & Gallagher, B. (1996). *Policing child sexual abuse: The view from police practitioners.* Home Office.

Hundley, V., Milne, J., Leighton-Beck, L., Graham, W., & Fitzmaurice, A. (2000). Raising research awareness among midwives and nurses: does it work? *Journal of Advanced Nursing*, *31*(1), 78-88.

Hurrell, A.K, Draycott, S., & Andrews L. (2017). Secondary traumatic stress in police officers investigating childhood sexual abuse. *Policing: An International* Journal Vol. 41 No5, 2018 pp.636-650. DOI: 10.1108/PIJPSM-08-2016-0131

Hutto, C. J., Bell, C., Farmer, S., Fausset, C., Harley, L., Nguyen, J., & Fain, B. (2015, January). Social media gerontology: Understanding social media usage among older adults. In *Web intelligence* (Vol. 13, No. 1, pp. 69-87). IOS Press.

Hyde, K.F. (2000), "Recognising deductive processes in qualitative research", *Qualitative Market Research*, Vol. 3 No. 2, pp. 82-90. https://doi.org/10.1108/13522750010322089

Independent Inquiry Child Sexual Abuse. The Internet Investigation Report (2020). (Online). Retrieved on February 23, 2021, from <a href="https://www.iicsa.org.uk/publications/investigation/internet">https://www.iicsa.org.uk/publications/investigation/internet</a>

Internet Growth Statistics 1995 to 2023, The Global Village. (Online). Retrieved on 15<sup>th</sup> April 2023 from: <a href="www.internetworldstats.com.stats4">www.internetworldstats.com.stats4</a>

Internet Watch Foundation. (2018). Trends in Online Child Sexual Exploitation: Examining the Distribution and Capture of Live Stream Sexual Abuse. (Online). Retrieved on 13<sup>th</sup> March 2023 from: <a href="https://www.iicsa.org.uk/key-docu-ments/15075/view/IWF000010.pdf">https://www.iicsa.org.uk/key-docu-ments/15075/view/IWF000010.pdf</a>

Internet Watch Foundation. (2020). The dark side of the selfie: IWF partners with the Marie Collins Foundation in a new campaign to call on young men to report self-generated sexual images of under 18s. (Online). Retrieved

fromhttps://www.iwf.org.uk/news/dark-side-of-selfie-iwf-partners-marie-collinsfoundation-new-campaign-to-call-on-young-men-to

Internet Watch Foundation. Our History. (Online). Retrieved on 7 October 2022 from: <a href="https://www.iwf.org.uk/about-us/who-we-are/annual-report-2021">https://www.iwf.org.uk/about-us/who-we-are/annual-report-2021</a>

Iqbal, M. (2003). Defining cyberterrorism. J. Marshall J. Computer & Info. L., 22, 397.

Isaacs Russell, G. (2020). Remote working during the pandemic: a Q&A with Gillian Isaacs Russell: Questions from the editor and editorial board of the BJP. *British Journal of Psychotherapy*, *36*(3), 364-374.

IWF (2019). Research on Live-streaming child sexual abuse. (Online). Retrieved on 24<sup>th</sup> March 2023 from <a href="https://www.iwf.org.uk/news-media/news/iwf-research-on-child-sex-abuse">https://www.iwf.org.uk/news-media/news/iwf-research-on-child-sex-abuse</a>.

IWF (2020) Live-Streaming Reports. (Online). Retrieved on 24<sup>th</sup> March 2023 from <a href="https://www.iwf.org.uk/news-media/news/our-live-streaming-report-the">https://www.iwf.org.uk/news-media/news/our-live-streaming-report-the</a>.

IWF (2022) Three-Fold Increase of Abuse Imagery of 7-10-Year-Olds as IWF Detect More Child Abuse than Ever Before Online. (Online). Retrieved on 17<sup>th</sup> March 2023 from: <a href="https://www.iwf.org.uk/news-media/news/three-fold-increase-of-abuse-imagery-of-7-10-year-olds-as-iwf-detects-more-child-sexual-abuse-material-online-than-ever-before/">https://www.iwf.org.uk/news-media/news/three-fold-increase-of-abuse-imagery-of-7-10-year-olds-as-iwf-detects-more-child-sexual-abuse-material-online-than-ever-before/</a>

IWF (2023). Eliminating Child Sexual Abuse. (Online). Retrieved on 28<sup>th</sup> March 2024 from: <a href="https://www.bing.com/ck/a?!&&p=e0283e55b7ad1e88Jmlt-dHM9MTcxMTU4NDAwMCZpZ3VpZD0w">https://www.bing.com/ck/a?!&&p=e0283e55b7ad1e88Jmlt-dHM9MTcxMTU4NDAwMCZpZ3VpZD0w</a>

Jackson, R. L. (1989). Child molesters use electronic networks: Computer-crime sleuths go undercover. *Los Angeles Times*, 20.

James, A., Rogers, C., Turner, J., & Silverstone, D. (2023). Helping the police with their inquiries: improving investigator resilience and capacity in England and Wales. *Journal of Criminological Research, Policy and Practice*.

Jamshed, S. (2014). Qualitative research method-interviewing and observation. *Journal of basic and clinical pharmacy*, *5*(4), 87.

Jewkes, Y., & Andrews, C. (2005) Policing the filth: The problems of investigating online child pornography in England and Wales, *Policing and Society*, 15:1, 42-62, DOI: 10.1080/1043946042000338922

Jewks, Y. (2010). Policing and Internet Crime. *In Y. Jewks and M. Yar, eds. Handbook of Internet Crime*. Cullompton; Willan, 245-265

Jiang, J. J., Muhanna, W. A., & Klein, G. (2000). User resistance and strategies for promoting acceptance across system types. *Information & Management*, *37*(1), 25-36.

Joffe, H. (2011). Thematic analysis. *Qualitative research methods in mental health and psychotherapy: A guide for students and practitioners*, 209-223.

Johnson, D., Faulkner, E., Meredith, G., & Wilson, T. J. (2020). Police functional adaptation to the digital or post-digital age: Discussions with cybercrime experts. *The Journal of Criminal Law*, *84*(5), 427-450.

Johnson, D., Faulkner, E., Meridith, G., & Wilson, T. (2020). Police Function Adaption to the Digital or Post Digital Age: Discussion with Cybercrime Experts. *The Journal of Criminal Law 2020*, Vol. 84(5) 427-450. DOI:10.177/0022018320952559

Johnson, M. (2010). Freedom of Expression in Cyberspace and the Coroners and Justice Act 2009. *An Information Law for the 21st Century*, 54.

Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come. *Educational researcher*, *33*(7), 14-26.

Johnston, M. P. (2014). Secondary data analysis: A method of which the time has come. *Qualitative and quantitative methods in libraries*, *3*(3), 619-626.

Joleby, M., Lunde, C., Landström, S., & Jonsson, L. S. (2021). Offender strategies for engaging children in online sexual activity. *Child Abuse & Neglect*, *120*, 105214.

Jones, E., & Chaplin, E. (2020). A systematic review of the effectiveness of psychological approaches in the treatment of sex offenders with intellectual disabilities. *Journal of Applied Research in Intellectual Disabilities*, *33*(1), 79-100

Jootun, D., McGhee, G., & Marland, G. R. (2009). Reflexivity: promoting rigour in qualitative research. *Nursing Standard*, *23*(23), 42-47.

Kaiser, J., & Rauchfleisch, A. (2019). *The implications of venturing down the rabbit hole. Internet Policy Review*, 8(2), 1–22.

Karasavva, V., & Noorbhai, A. (2021). The real threat of deepfake pornography: A review of Canadian policy. *Cyberpsychology, Behavior, and Social Networking, 24*(3), 203-209.

Katz, J. (2015). A theory of qualitative methodology: The social system of analytic fieldwork. *Méthod (e) s: African Review of Social Sciences Methodology, 1*(1-2), 131-146.

Kemp, S. (2022). Data Reportal. (Online). Accessed on 10<sup>th</sup> June 2024 from <a href="https://data-reportal.com/reports/digital-2022-favorite social media platforms.">https://data-reportal.com/reports/digital-2022-favorite social media platforms.</a>

Kemp, S. (2019) Digital 2019: *Global internet use accelerates; we are social,* 30 January 2019. https://wearesocial. Com/blog/2019/01/digital-2019-global-internet-use accelerates

Keyes, C. F. (2002). Weber and anthropology. *Annual Review of Anthropology*, *31*(1), 233-255.

Khader, M. (Ed.). (2016). *Combating violent extremism and radicalization in the digital era*. IGI Global.

Khasawneh, A., Chalil Madathil, K., Dixon, E., Wiśniewski, P., Zinzow, H., & Roth, R. (2020). Examining the self-harm and suicide contagion effects of the Blue Whale Challenge on YouTube and Twitter: qualitative study. *JMIR mental health*, 7(6), e15973.

Kiecolt, K. Jill, David Brinberg, Katrin Auspurg, Laura E. Nathan, and Laura E. Nathan. *Secondary analysis of survey data*. Vol. 53. Sage, 1985.

Kierkegaard, S. (2011). To block or not to block–European child porno law in question. *Computer Law & Security Review, 27*(6), 573-584.

Kim, J. F. (2018). Break the deadlock. *Contemporary Literary Review India, 5*(4), 101-112.

Kinitz, D. J. (2022). The emotional and psychological labor of insider qualitative research among systemically marginalized groups: Revisiting the uses of reflexivity. *Qualitative Health Research*, *32*(11), 1635-1647.

King, N. (2004). Using templates in thematic analysis of text. In C. Cassell & G. Symonds (Eds.) *Essential guide to qualitative methods in organisational research* (pp. 257-270). London, UK: Sage

Kip, H., Kelders, S. M., Weerink, K., Kuiper, A., Brüninghoff, I., Bouman, Y. H., ... & van Gemert-Pijnen, L. J. (2019). Identifying the added value of virtual reality for treatment in forensic mental health: a scenario-based, qualitative approach. *Frontiers in Psychology*, *10*, 406.

Kirby, S. (2018). Can University Graduates really become police detectives in 12 weeks? The jury's still out. <a href="https://researchgate.net/publication/355649584">https://researchgate.net/publication/355649584</a>.

Kirwan, G., & Power, A. (2013). *Cybercrime: The psychology of online offenders*. Cambridge University Press.

Kleijn, M., & Bogaerts, S. (2021). Sexual offending pathways and chat conversations in an online environment. *Sexual Abuse*, *33*(8), 871-890.

Kleinrock, L. (2010). An early history of the internet [History of Communications]. *IEEE Communications Magazine*, *48*(8), 26-36.

Klettke, B., Hallford, D. J., & Mellor, D. J. (2014). Sexting prevalence and correlates: A systematic literature review. *Clinical psychology review*, *34*(1), 44-53.

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

Kloess, J. A., Woodhams, J., Whittle, H., Grant, T., & Hamilton-Giachritsis, C. E. (2019). The Challenges of Identifying and Classifying Child Sexual Abuse Material. *Sexual Abuse*, *31*(2), 173–196. https://doi.org/10.1177/1079063217724768

Knott, E., Rao, A.H., Summers, K. *et al.* Interviews in the social sciences. *Nat Rev Methods Primers* **2**, 73 (2022). https://doi.org/10.1038/s43586-022-00150-6

Koller, V. (2009). Analysing collective identity in discourse: social actors and contexts. [Texte anglais original]. *Semen. Revue de sémio-linguistique des textes et discours,* (27).

Koper, C. S., Lum, C., & Willis, J. J. (2014). Optimising the use of technology in policing: Results and implications from a multi-site study of the social, organisational, and behavioural aspects of implementing police technologies. *Policing: A Journal of Policy and Practice*, *8*(2), 212-221.

Koverola, C., & Foy, D. (1993). Post-traumatic stress disorder symptomatology in sexually abused children: Implications for legal proceedings. *Journal of Child Sexual Abuse*, 2, 119–127.

Krone, T. (2004) A Typology of Online Child Pornography Offending. *Trends and issues in crime and criminal justice*, No. 279. Australian Institute of Criminology.

Krone, T. (2005). Queensland police stings in online chat rooms. *Trends and issues in crime and criminal justice*, (301), 1-6.

Kruithof, K., Aldridge, J., Décary-Hétu, D., Sim, M., Dujso, E., & Hoorens, S. (2016). Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands.

Kula, S. (2017). Occupational Stress, supervisor support, job satisfaction, and work-related burnout: Perceptions of Turkish National Police (TNP) members. *Police Practice and Research*, 18(2), 146-159

Kulibert, D., Moran, J. B., Preman, S., Vannier, S. A., & Thompson, A. E. (2021). Sex on the screen: A content analysis of free internet pornography depicting mixed-sex threesomes from 2012–2020. *European journal of investigation in health, psychology and education, 11*(4), 1555-1570.

Kuter, U., & Yilmaz, C. (2001). Survey methods: Questionnaires and interviews. *Choosing Human-Computer Interaction (HCI) Appropriate Research Methods*.

Laird, J. J., Klettke, B., Hall, K., Clancy, E., & Hallford, D. (2020). Demographic and psychosocial factors associated with child sexual exploitation: A systematic review and meta-analysis. *JAMA network open*, *3*(9), e2017682-e2017682.

Larricchia, F. (2023). Children owning mobile phones in the UK, 2023, by age. (Online). Retrieved on 17<sup>th</sup> July 2024 from <a href="https://statista.com/statistics/1326211/children-owning-mobile-telephones-by-age">https://statista.com/statistics/1326211/children-owning-mobile-telephones-by-age</a>

Landrum, B. J. (1998). Marketing innovations to nurses, Part 2: Marketing's role in the adoption of innovations. *Journal of WOCN*, *25*(5), 227-232.

Lane, F.S. (2000). *Obscene profits: The entrepreneurs of pornography in the cyber age.* Routledge.

Lane, T. D. (2000). *Machine learning techniques for the computer security domain of anomaly detection*. Purdue University.

Langford, D. (Ed.). (2000). *Internet ethics*. London: Macmillan.

Lanier, J. (2018). *Ten arguments for deleting your social media accounts right now.* Random House.

Lanning, K. V. (2001). Child molesters: A behavioral analysis. *For law enforcement officers investigating the sexual exploitation of children by acquaintance molesters*, 2-86.

Lanning, K. V., & Burgess, A. W. (1984). *Child pornography and sex rings* (Vol. 8). Federal Bureau of Investigation, U.S. Department of Justice.

Lanning, K.V. (2010). Child molesters: A behavioural analysis for professionals investigating the sexual exploitation of children. (Online). Retrieved on 2<sup>nd</sup> June 2021, from <a href="https://calio.org/wp-content/uploads/2020/03/Child-Molesters-A-Behavioral-Analysis.pdf">https://calio.org/wp-content/uploads/2020/03/Child-Molesters-A-Behavioral-Analysis.pdf</a>

Laufs J, Waseem Z. Policing in pandemics: A systematic review and best practices for police response to COVID-19. *Int J Disaster Risk Reduct.* 2020 Dec;51:101812. doi: 10.1016/j.ijdrr.2020.101812. Epub 2020 Aug 20. PMID: 32839687; PMCID: PMC7439012.

Laycock, G. (2001). *Research for police: Who needs it?* (Vol. 211). Canberra, Australia: Australian Institute of Criminology.

Leal, J. (2009). E-learning and online education: Implications for the future of law enforcement training. *World Future Review, 1*(3), 22-28.

Leander, L., Christianson, S. Å., & Granhag, P. A. (2008). Internet-initiated sexual abuse: adolescent victims' reports about On-and Offline sexual activities. *Applied Cognitive Psychology: The Official Journal of the Society for Applied Research in Memory and Cognition, 22*(9), 1260-1274.

Lee, H. E., Ermakova, T., Ververis, V., & Fabian, B. (2020). Detecting child sexual abuse material: A comprehensive survey. *Forensic Science International: Digital Investigation*, *34*, 301022.

Lee, H. Y., Jamieson, J. P., Reis, H. T., Beevers, C. G., Josephs, R. A., Mullarkey, M. C., ... & Yeager, D. S. (2020). Getting fewer "likes" than others on social media elicits emotional distress among victimized adolescents. *Child Development*, *91*(6), 2141-2159.

Lee, T. T. (2004). Nurses' adoption of technology: application of Rogers' innovation-diffusion model. *Applied nursing research*, *17*(4), 231-238.

Legistaltion.Gov. Obscene Publications Act 1959. (Online). Retrieved on 22<sup>nd</sup> August 2022 from <a href="https://www.legislation.gov.uk/ukpga/Eliz2/7-8/66/contents">https://www.legislation.gov.uk/ukpga/Eliz2/7-8/66/contents</a>

Lekan-Rutledge, D. (2000). Diffusion of innovation: a model for implementation of prompted voiding in long-term care settings. *Journal of Gerontological Nursing*, *26*(4), 25-33.

Leo, R.A, & Ofshe, R.J. (1998). The consequences of false confessions: Deprivation of liberty and miscarriages of justice in the age of psychological interrogation. *Journal of Criminal Law and Criminology, 88, 429-496.* 

Leonhardt, M., & Overå, S. (2021). Are there differences in video gaming and use of social media among boys and girls?—A mixed methods approach—international journal of environmental research and public health, 18(11), 6085.

Leukfeldt, R, Veenstra, S, & Wouter, S. (2013), High Volume CyberCrime and the Organization of the Police: The results of two empirical studies in the Netherlands. *International Journal of Cyber Criminology*, Vol 7, Issue 1, January – June 2013.

Li, J.X., (2017). Cyber Crime and Legal Countermeasures: A Historical Analysis. *International Journal of Criminal Justice Sciences*, 12(2)

Liang, H., Xue, Y., & Byrd, T. A. (2003). PDA usage in healthcare professionals: testing an extended technology acceptance model. *International Journal of Mobile Communications*, *1*(4), 372-389.

Liberatore, M., Erdely, R., Kerle, T., Levine, B. N., & Shields, C. (2010). Forensic investigation of peer-to-peer file sharing networks. *digital investigation*, *7*, S95-S103.

Lifewire (2019). What is a Cyberlocker? (Online). Retrieved on 5<sup>th</sup> April 2023 from: <a href="https://www.lifewire.com/what-is-a-cyberlocker-2483215">https://www.lifewire.com/what-is-a-cyberlocker-2483215</a>

Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry. Sage.

Lindsay, R., Jackson, T. W., & Cooke, L. (2011). Adapted technology acceptance model for mobile policing. *Journal of Systems and Information Technology*. 13(4), pp.389-407.

Lingard, L., Albert, M., & Levinson, W. (2008). Grounded theory, mixed methods, and action research. *Bmj*, *337*.

Lipscomb, M. (2012). Abductive reasoning and qualitative research. *Nursing philoso- phy, 13*(4), 244-256.

Livingstone, S. (2001). Online freedom and safety for children. (Online). Retrieved on March 24, 2023, from: <a href="http://eprints.lse.ac.uk/id/eprint/416">http://eprints.lse.ac.uk/id/eprint/416</a>

Livingstone, S., & Brake, D. R. (2010). On the rapid rise of social networking sites: New findings and policy implications. *Children & Society, 24*(1), 75-83.

Livingstone, S., Davidson, J., Bryce, J., Batool, S., Haughton, C., & Nandi, A. (2017). Children's online activities, risks and safety: a literature review by the UKCCIS evidence group.

Loewenstein, G., & Lerner, J. S. (2003). The role of affect in decision making. In R. J. Davidson, K. R. Scherer, & H. H. Goldsmith (Eds.), Handbook of affective sciences (pp. 619-642). Oxford, UK: Oxford University Press.

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

Long, M., Alison, L., Tejeriro, R., Giles, S., & Hendricks, E. (2016). Kirat: Law Enforcement's Prioritisation Tool for Investigating indecent image Offenders. *Psychology, Public Policy and Law,* 2016, Vol, 22, No 1, 12-21: Doi: 10.1037/law000069

Loveday, B. (2017). Still plodding along? The police response to the changing profile of crime in England and Wales. *International Journal of Police Science &* 

Management, 19(2), 101-109. https://doi.org/10.1177/1461355717699634

Lukosch, H., & de Vries, P. (2009). Supporting informal learning at the workplace. *International Journal of Advanced Corporate Learning (iJAC)*, *2*(3), 39-44.

Lum, C. (2010). Technology and mythology of progress in American law enforcement. *Science Progress*, *8*, 12.

Maddocks. S. (2020). "'A Deepfake Porn Plot Intended to Silence Me': exploring continuities between pornographic and 'political deep fakes." *Porn Studies* 7, no. 4: 415-423.

Madigan, S., Ly, A., Rash, C. L., Van Ouytsel, J., & Temple, J. R. (2018). Prevalence of multiple forms of sexting behavior among youth: A systematic review and meta-analysis. *JAMA pediatrics*, *172*(4), 327-335.

Magnusson, S.J., Palincsar, A.S., Hapgood, S., & Lomangino, A. (2004). How should learning be structures in inquiry-based science instruction? Investigating the interplay of 1st- and 2nd-hand investigations. In Y. Kafai, W. Sandoval, N. Enyedy, A. Nixon, & F. Herrera (Eds.), Proceedings of the Sixth International Conference of the Learning Sciences (pp. 310–317).

Maher, C., Hadfield, M., Hutchings, M., & de Eyto, A. (2018). Ensuring Rigor in Qualitative Data Analysis: A Design Research Approach to Coding Combining NVivo With Traditional Material Methods. *International Journal of Qualitative Methods*, 17(1). <a href="https://doi.org/10.1177/1609406918786362">https://doi.org/10.1177/1609406918786362</a>

Mahmud, B. U., & Sharmin, A. (2021). Deep insights of deepfake technology: A review. *arXiv preprint arXiv:2105.00192*.

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

Mandau, M. B. H. (2021). "Snaps", "screenshots", and self-blame: A qualitative study of image-based sexual abuse victimization among adolescent Danish girls. *Journal of Children and Media*, *15*(3), 431-447.

Mann, N., Devendran, P., & Lundrigan, S. (2020). Monitoring Officers, *Policing: A Journal of Policy and Practice*, Volume 14, Issue 3, September 2020, Pages 630–642, https://doi.org/10.1093/police/pay047

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

Marcum, C. D., Higgins, G. E., Freiburger, T. L., & Ricketts, M. L. (2010). Policing possession of child pornography online: Investigating the training and resources dedicated to the investigation of cybercrime. *International Journal of Police Science & Management*, *12*(4), 516-525.

Markus, M. L. (1983). Power, politics, and MIS implementation. *Communications of the ACM*, *26*(6), 430-444.

Marras, M.H., & Shapiro, L.R. (2017). Child sex dolls and robots: More than just an uncanny valley. *Journal of Internet Law, 2017 (x), 1-21* 

Martellozzo, E., & Bradbury, P. (2021). How the Pandemic has made young people more vulnerable to risky online sexual trade. *Parenting for a Digital Future*.

Martin, G. (2006). Understanding Terrorism: Challenges, Perspectives, and Issues Second Edition.

Martin, J. (2014). *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs.* Springer.

Marwick, A., Fontaine, C., & Boyd, D. (2017). "Nobody sees it, nobody gets mad": social media, privacy, and personal responsibility among low-SES youth. *Social media+ Society, 3*(2), 2056305117710455

Mathers, N. J., Fox, N. J., & Hunn, A. (1998). *Surveys and questionnaires* (Vol. 1998). NHS Executive, Trent.

Mauthner NS, & Doucet A (2003) Reflexive accounts and accounts of reflexivity in qualitative data analysis. *Sociology*. 37, 3, 413-431

Maxwell, J. A. (2006). *Qualitative Research Design: An Interactive Approach* (2nd ed.). Thousand Islands: Sage.

Maxwell, J. A. (2012). A realist approach for qualitative research. Sage.

McAlinden, A. M. (2012). *'Grooming' and the Sexual Abuse of Children: Institutional, Internet and Familial Dimensions*. Oxford University Press.

McAlister, R. (2014). New Technologies, 'Risk' and Sexual Offending. In: McCartan, K. (eds) Responding to Sexual Offending. Palgrave Studies in Risk, Crime and Society. Palgrave Macmillan, London. https://doi.org/10.1057/9781137358134\_4

McCarthy, D., & O'Neill, M. (2014). The police and partnership working reflections on recent research. *Policing: A Journal of Policy and Practice*, 8(3), 243-253.

McCarthy, J. A. (2010). Internet sexual activity: A comparison between contact and non-contact child pornography offenders. *Journal of sexual aggression*, *16*(2), 181-195.

McCrudden, M. T., & McTigue, E. M. (2019). Implementing integration in an explanatory sequential mixed methods study of belief bias about climate change with high school students. *Journal of Mixed Methods Research*, *13*(3), 381-400.

McEwen, T. (2003). Evaluation of the Locally Initiated Research Partnership Program. Washington, DC: National Institute of Justice.

McGloin, S. (2008). The trustworthiness of case study methodology. *Nurse Researcher*, 16(1), 45-55. doi: 10.7748/nr2008.10.16.1.45.c6752

McGlynn, C., & Bows, H. (2019). Possessing extreme pornography: Policing, prosecutions and the need for reform. *The Journal of Criminal Law, 83*(6), 473-488.

McGuire, M. (2012). *Technology, crime and justice: the question concerning technomia. Willan.* 

McGuire, M. (2019). It ain't what it is, it's the way that they do it. Why we still don't understand cybercrime. In *The human factor of cybercrime* (pp. 3-28). Routledge.

McGuire, M. (2021) *The Human Factors of Cybercrime* (2021). In Leukfeldt, R., & Holt, J. (Eds). *The Human Factors of Cybercrime* (pp 14). Routledge. Taylor and Francis Group

McIntosh, M. J., & Morse, J. M. (2015). Situating and constructing diversity in semi-structured interviews. *Global qualitative nursing research*, *2*, 2333393615597674.

McLaughlin, J. F. (2000). Cyber child sex offender typology. *Knight Stick: Publication of the New Hampshire Police Association*, *51*, 39-42.

Mclean, N., & Marshall, L. A. (2010). A front-line police perspective of mental health issues and services. *Criminal behaviour and mental health, 20*(1), 62-71.

McLelland, Mark (2012) 'Australia's Child-Abuse Materials Legislation, Internet Regulation, and the juridification of the Imagination,' *International Journal of Cultural Studies*, 15(5): 467-83.

McLelland, M., (2017) 'Negotiating 'Cool Japan' in Research and Teaching,' in Mark McLelland (ed.), The End of Cool Japan: Ethical, Legal and Cultural Challenges to Japanese Popular Culture, Oxon: Routledge, pp. 1-30.

McManus, Long and Alison (2011). Kent Internet Risk Assessment Tool. (Online). Retrieved on 17<sup>th</sup> March 2022 from <a href="https://www.rma.scot/wp-content/up-loads/2019/09/RATED\_KIRAT\_August-2019\_Hyperlink-Version.pdf">https://www.rma.scot/wp-content/up-loads/2019/09/RATED\_KIRAT\_August-2019\_Hyperlink-Version.pdf</a>

Metcalf, C. (2007). Policing operation ore.

Mead, G. H. (1934). *Mind, self, and society* (Vol. 111). Chicago: University of Chicago Press.

Meeus, A., Beullens, K., & Eggermont, S. (2019). Like me (please?): Connecting online self-presentation to pre- and early adolescents' self-esteem. *New Media & Society, 21*(11–12), 2386–2403. <a href="https://doi.org/10.1177/1461444819847447">https://doi.org/10.1177/1461444819847447</a>

Meijer, A., Lorenz, L., & Wessels, M. (2021). Algorithmization of bureaucratic organizations: Using a practice lens to study how context shapes predictive policing systems. *Public Administration Review*, *81*(5), 837-846.

Merdian, H. L., Wilson, N., & Boer, D. P. (2009). Characteristics of internet sexual offenders: A review. *Sexual Abuse in Australia and New Zealand*, *2*(1), 34-47.

Merola, L. M., Lum, C., Cave, B., & Hibdon, J. (2014). Community support for license plate recognition. *Policing: An International Journal of Police Strategies & Management*.

Metro (2022). Rise in children filming their own sexual abuse. (Online). Retrieved on 10<sup>th</sup> April 2023 from: metro.co.uk/2022/08/09/disturbing-rise-in-children-filming-their-own-sexual-abuse

Metropolitan Police (2023) Detective Training. (Online) Retrieved on 22<sup>nd</sup> February 2023 from <a href="https://www.met.police.uk/.../detective-constable/training-and-benefits">https://www.met.police.uk/.../detective-constable/training-and-benefits</a>

Microsoft (2022). PhotoDNA. (Online). Retrieved on 18<sup>th</sup> May 2023 from <a href="https://www.microsoft.com/en-us/photodna">https://www.microsoft.com/en-us/photodna</a>

Mills, (2014). Methodology and methods. In Jane Mills & Melanie Birks (Eds.), Qualitative methodology: A practical guide (pp.31-47). Thousand Oaks, CA: Sage.

Milgram, S. (1963). Behavioral study of obedience. *The Journal of abnormal and social psychology*, *67*(4), 371.

Milivojevic, S. (2021). *Crime and Punishment in the Future Internet: Digital Frontier Technologies and Criminology in the Twenty-First Century.* Routledge.

Mitchell, K. J., Finkelhor, D., Jones, L. M., & Wolak, J. (2010). Use of social networking sites in online sex crimes against minors: An examination of national incidence and means of utilization. *Journal of Adolescent Health*, *47*(2), 183-190.

Mitchell, K. J., Jones, L. M., Finkelhor, D., & Wolak, J. (2011). Internet-facilitated commercial sexual exploitation of children: Findings from a nationally representative sample of law enforcement agencies in the United States. *Sexual Abuse*, *23*(1), 43-71.

Mitchell, K.J., Finkelhor, D., Jones, L.M., & Wolak, J. (2010). Growth and change in undercover online child exploitation investigations, 2000 to 2006. *Policing & Society*, 20(4), 416–431.

Mohamed, A., & Ismail, I. (2022). A performance comparative on most popular internet web browsers. *Procedia Computer Science*, *215*, 589-597.

Money, W., & Turner, A. (2004, January). Application of the technology acceptance model to a knowledge management system. In *37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the* (pp. 9-pp). IEEE.

Morgan, D. L. (2007). Paradigms lost, and pragmatism regained: Methodological implications of combining qualitative and quantitative methods. *Journal of mixed methods research*, *1*(1), 48-76.

Morris, E. (2020). "Children: extremism and online radicalization." *Journal of Children and Media* 10, no. 4: 508-514.

Morris, M. G., & Venkatesh, V. (2000). Age differences in technology adoption decisions: Implications for a changing work force. *Personnel psychology*, *53*(2), 375-403.

Muller, E.R., Rosenthal, U. en E.J. van der Torre (eds) Politie: studies over haar werking en organizatie, Deventer: Kluwer

Najdowski, C. 2017. "Legal Responses to Nonconsensual Pornography: Current Policy in the United States and Future Directions." *Psychology, Public Policy and Law* 23 (2):154–65. doi: 10.1037/law0000123

Napier, S., Boxall, H., & Teunissen, C. (2021). Live streaming of child sexual abuse: An analysis of offender chat logs. *Trends and Issues in Crime and Criminal Justice [electronic resource]*, (639), 1-15.

Napier, S., Cubitt, T., & Brown, R. (2021). Predicting prolific live streaming of child sexual abuse. *Trends and Issues in Crime and Criminal Justice [electronic resource]*, (634), 1-21.

Napier, S., Smith, R. G., & Brown, R. (2020). Australians who view live streaming of child sexual abuse: An analysis of financial transactions. *Trends and Issues in Crime and Criminal Justice [electronic resource]*, (589), 1-16.

Napier, S., Teunissen, C., & Boxall, H. (2021). How do child sexual abuse live streaming offenders access victims? *Trends and Issues in Crime and Criminal Justice [electronic resource]*, (642), 1-18.

Naso, C. (2011). Sext Appeals: Re-Assessing the Exclusion of Self-Created Images from First Amendment Protection. *Crim. L. Brief, 7,* 4.

National Centre for Missing and Exploited Children (2020). (Online). Retrieved on 21<sup>st</sup> March 2023 from <a href="http://www.ncmec.org/">http://www.ncmec.org/</a>

National Centre for Missing and Exploited Children (2021). Reports by Electronic Service Providers. (Online). Retrieved on 24<sup>th</sup> August 2022 from <a href="https://www.missing-kids.org/content/dam/missingkids/pdfs/2021-reports-by-esp.pdf">https://www.missing-kids.org/content/dam/missingkids/pdfs/2021-reports-by-esp.pdf</a>

National Education Union (2021). Sexting Incidents in School. (Online). Retrieved on Jan 20, 2022, from <a href="https://neu.org.uk/advice/sexting-incidents-school">https://neu.org.uk/advice/sexting-incidents-school</a>

Naylor, J. (2004). Gregory J. Downey—Telegraph Messenger Boys: Labor, Technology, and Geography, 1850-1950. *Histoire sociale/Social History*.

NCPCC (2019). 200,000 Young People May Have Been Groomed on Social Media. (Online). Retrieved on 21st March 2023 from <a href="https://www.nspcc.org.uk/about-us/news-opinion/2019/over-5000-grooming-offences-recorded-18-months/">https://www.nspcc.org.uk/about-us/news-opinion/2019/over-5000-grooming-offences-recorded-18-months/</a>

Nee, C., Gelder, J., Otte, M., Vernham, Z., & Meenaghan, A. (2019). Learning on the job: Studying expertise in residential burglars using virtual environments\*. Criminology; An Interdisciplinary Journal, 1745-9125.12210, doi:10.1111/1745-9125.12210

Nelson, R. (2014). *What does the Polygraph Measure? APA Magazine 2014.* Retrieved on 9th October 2019 from <a href="https://www.getsafeonline.org/news/nca-warning-about-sex-of-fenders-use-of-live-streaming-platforms/">https://www.getsafeonline.org/news/nca-warning-about-sex-of-fenders-use-of-live-streaming-platforms/</a>

Nutbrown, B., Scholey, E., Baldi, P., McKeown, K., Swanson, A., Bardill, R. (2019). Social Media, Television and Children. Sheffield: University of Sheffield.

Nesi, J., Choukas-Bradley, S., Maheux, A. J., Roberts, S. R., Sanzari, C. M., Widman, L., & Prinstein, M. J. (2021). Selfie appearance investment and peer feedback concern: Multimethod investigation of adolescent selfie practices and adjustment. *Psychology of Popular Media*, *10*(4), 488.

Neuendorf, K. A. (2017). The content analysis guidebook. Sage.

Neumann, M. M., & Herodotou, C. (2020). Evaluating YouTube videos for young children. *Education and Information Technologies*, *25*, 4459-4475.

Nicol, S. J., Harris, D. A., Kebbell, M. R., & Ogilvie, J. (2021). Online Child Sexual Exploitation Material: A Comparison From Police Data on Men Charged With Child Sexual Exploitation Material Exclusively and Men Charged With Contact Child Sexual Abuse Exclusively. *Sexual Offending: Theory, Research, and Prevention, 16,* 1-18.

Nikolić, G. (2020). NATIONAL CRIME AGENCY-NCA. *International Journal of Economics & Law, 10*(30), 17-30.

Norton (2023). What is bulletproof hosting? (Online). Retrieved on 17<sup>th</sup> April 2023 from: <a href="https://us.norton.com/blog/emerging-threats/what-is-bulletproof-hosting">https://us.norton.com/blog/emerging-threats/what-is-bulletproof-hosting</a>

Nowell, LS., Norris, JM., White, DE, & Moules NJ. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. *International Journal of Qualitative Methods*, Volume 16:1-13 DOI: 10.1177/1609406917733847

NSPCC (2021). Sexting Advice for Professionals. (Online). Retrieved on Jan 21, 2022, from <a href="https://learning.nspcc.org.uk/research-resources/briefings/sexting-advice-profession-als">https://learning.nspcc.org.uk/research-resources/briefings/sexting-advice-profession-als</a>.

NSPCC (2022). Live streaming and video apps. (Online). Retrieved on 8<sup>th</sup> November 2022 from: https://www.nspcc.org.uk/.../online-safety/livestreaming-online-video-apps

Nunkoosing, K. (2005). The problems with interviews. *Qualitative health research*, *15*(5), 698-706.

O'Brien, M. D., & Webster, S. D. (2007). The construction and preliminary validation of the Internet Behaviours and Attitudes Questionnaire (IBAQ). *Sexual Abuse*, *19*(3), 237-256.

Odag, Ö., Leiser, A., & Boehnke, K. (2019). Reviewing the role of the Internet in radicalization processes. *Journal for deradicalization*, (21), 261-300.

Ofcom (2022). What is Ofcom? (Online). Retrieved on 4<sup>th</sup> November 2023 from <a href="https://www.ofcom.org.uk/about-ofcom/what-is-ofcom/what-

Ofcom (2022). Why Children spend time online. (Online). Retrieved on 2 February 2022 from:protectyourkids.org.uk/2019/01/new-Ofcom-report-reveals-why-children-are-spending

Ofcom (2022). Children and Parents Media Use and Attitudes Report. (Online). Retrieved on 8<sup>th</sup> April 2023 from: <a href="https://www.ofcom.org.uk/research-and-data/media-literacy-research/">https://www.ofcom.org.uk/research-and-data/media-literacy-research/</a>

Ogburn, W. F. (1964). *William F. Ogburn on culture and social change*. University of Chicago Press.

Olson, L. N., Daggs, J. L., Ellevold, B. L., & Rogers, T. K. (2007). Entrapping the innocent: Toward a theory of child sexual predators' luring communication. *Communication Theory*, *17*(3), 231-251.

Online Abuse, House of Commons (2022). (Online) Retrieved on 14<sup>th</sup> March 2023 from: <a href="https://www.local.gov.uk/.../online-abuse-house-commons-28-february-2022">https://www.local.gov.uk/.../online-abuse-house-commons-28-february-2022</a>

Onwuegbuzie, A. J., Bustamante, R. M., & Nelson, J. A. (2010). Mixed research as a tool for developing quantitative instruments. *Journal of mixed methods research*, *4*(1), 56-78.

O'Shaughnessy R.J. Violent adolescent sexual offenders. Child Adolesc Psychiatr Clin N Am. 2002;11:749–65.

Owen, G., & Savage, N. (2015). The Tor Dark Net (2015). *Global Commission for Internet Governance,* Paper Series No 20.

Ozuem, W., Willis, M., & Howell, K. (2022). Thematic analysis without paradox: sensemaking and context. *Qualitative Market Research: An International Journal*, *25*(1), 143-157.

Page, E. B. (1966). Reviews: Webb, Eugene J., Campell, Donald T., Schwart, Richard D., and Sechrest, Lee. Unobtrusive Measures: Nonreactive Research in the Social Sciences. Chicago: Rand McNally, 1966. Paper, 225 pp. *American Educational Research Journal*, *3*(4), 317-319.

Päivi, Y. (2008) Perspectives into learning at the workplace. Educational Research Review 3 pp. 130-154. (doi:10.1016/j.edurev.2007.12.001)

Pannucci, C. J., & Wilkins, E. G. (2010). Identifying and avoiding bias in research. *Plastic and reconstructive surgery*, *126*(2), 619.

Paoline, A.E, Terrill, W., & Rossler, M.T. (2015) Higher Education, College Degree Major, and Police Occupational Attitudes, *Journal of Criminal Justice Education*, 26:1, 49-73, DOI: 10.1080/10511253.2014.923010

Paquette, S., Fortin, F., & Perkins, D. (2020). Online sexual offenders: typologies, assessment, treatment, and prevention. *The Wiley handbook of what works with sexual offenders: contemporary perspectives in theory, assessment, treatment, and prevention*, 311-326.

Parker, D. B. (1989). Computer Crime: *Criminal Justice Resource Manual*. National Institute of Justice.

Parker, D. B., & Parker, D. B. (1976). *Crime by computer* (pp. xii-xii). New York: Scribner.

Parkes, R., Graham-Kevan, N., & Bryce, J. (2019). You don't see the world through the same eyes anymore: the impact of sexual offending work on police staff. *The Police Journal*, *92*(4), 316-338.

PC Mag (2023). (Online) Retrieved on 5<sup>th</sup> April 2023 from:

https://www.pcmag.com/encyclopedia/term/internet-forum

Peersman, C., Schulze, C., Rashid, A., Brennan, M., & Fischer, C. (2016). iCOP: Live forensics to reveal previously unknown criminal media on P2P networks. *Digital Investigation*, *18*, 50-64.

Penfield, T., Baker, M. J., Scoble, R., & Wykes, M. C. (2014). Assessment, evaluations, and definitions of research impact: A review. *Research evaluation*, *23*(1), 21-32.

Penn, R., Rose, M., & Rubery, J. (Eds.). (1994). Skill and occupational change. OUP Oxford.

Pereira, M., Dodhia, R., Anderson, H., & Brown, R. (2020). Metadata-based detection of child sexual abuse material. *arXiv preprint arXiv:2010.02387*.

Pew Research Centre (2022). Teens, Social Media and Technology. (Online). Retrieved on 17<sup>th</sup> March 2023 from: www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-

Phippen, A., & Bond, E. (2024). Why do legislators keep failing victims in online harms? *International Review of Law, Computers & Technology*, 1-20.

Pires, F., Masanet, M. J., & Scolari, C. A. (2021). What are teens doing with YouTube? Practices uses and metaphors of the most popular audio-visual platform. *Information, Communication & Society, 24*(9), 1175-1191.

Platt, J. (1981). *The Social Construction of Positivism and its Significance in British Sociology, 1950-80.* 1st Ed. Routledge.

Police Federation of England and Wales Officer Demand Survey (2016). (Online). Retrieved on 1 October 2021 from <a href="https://www.polfed.org/our-work/demand-capacity-and-welfare/2016-survey-results/">https://www.polfed.org/our-work/demand-capacity-and-welfare/2016-survey-results/</a>

Police Workforce England and Wales: 31st March 2021 (Second Edition. (Online). Retrieved on 24th February 2023 from: https://www.gov.uk/.../police-workforce-england-

Polit, D. F., & Beck, C. T. (2010). Generalization in quantitative and qualitative research: Myths and strategies. *International journal of nursing studies, 47*(11), 1451-1458.

Pollitt, M. M. (1997). "Cyber terrorism fact or fancy?" Proceedings of the 20<sup>th</sup> National Information Sytems Security Conference, pp 285-9

Politics (2023). (Online). Retrieved on 6<sup>th</sup> November 2023 from <a href="https://www.politics.co.uk/references">https://www.politics.co.uk/references</a>

Popper, K. R. (2002). *An unended quest*. Psychology Press.

Potter, J., & Hepburn, A. (2005). Qualitative interviews in psychology: Problems and possibilities. *Qualitative research in Psychology*, *2*(4), 281-307.

Powell, A. (2007). *Paedophiles, child abuse and the internet: A practical guide to identification, action and prevention.* Radcliffe Publishing.

Prensky, M. (2005). Digital natives, digital immigrants. *Gifted*, (135), 29-31.

Priebe, G., & Svedin, C. G. (2008). Child sexual abuse is largely hidden from the adult society. An epidemiological study of adolescents' disclosures. *Child Abuse & Neglect*, 32(12), 1095–1108. doi:10.1016/j.chiabu.2008.04.001

Prus, R. (1996). *Symbolic interaction and ethnographic research*. Albany: State University of New York Press

Public Technology Net. (2019). All Police Forces Create Cybercrime Units. (Online). Retrieved on 24<sup>th</sup> February 2023, from <a href="https://www.publictechnology.net/articles/news/all-police-forces">https://www.publictechnology.net/articles/news/all-police-forces</a>

Pumpian, I., Fisher, D., Certo, N. J., & Smalley, K. A. (1997). Changing jobs: An essential part of career development. *Mental Retardation*, *35*(1), 39-48.

Punyanunt-Carter, N. M., & Wagner, T. R. (2018). Interpersonal communication motives for flirting face to face and through texting. *Cyberpsychology, Behavior, and Social Networking*, *21*(4), 229-233.

Pyett, P. M. (2003). Validation of qualitative research in the "real world". *Qualitative health research*, *13*(8), 1170-1179.

Quayle, E. (2020). Prevention, disruption and deterrence of online child sexual exploitation and abuse. In *ERA Forum* (Vol. 21, No. 3, pp. 429-447). Springer Berlin Heidelberg.

Quayle. E. (2022). Self-produced images, sexting, coercion and children's rights. *ERA Forum*. <a href="https://doi.org/10.1007/s12027-022-00714-9">https://doi.org/10.1007/s12027-022-00714-9</a>

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

Quayle, E., & Taylor, M. (2011). Social networking as a nexus for engagement and exploitation of young people. *Information security technical report*, *16*(2), 44-50.

Quinn, J. F., & Forsyth, C. J. (2013). Red light districts on blue screens: A typology for understanding the evolution of deviant communities on the internet. *Deviant Behavior*, *34*(7), 579-585.

Quinn, J.F, & Forsyth, C.J. (2005). Describing sexual behaviour in the era of the internet: A typology for empirical research. *Deviant behaviour, 26, 191-207* 

Quintão, C., Andrade, P., & Almeida, F. (2020). How to Improve the Validity and Reliability of a Case Study Approach? *Journal of Interdisciplinary Studies in Education*, *9*(2), 264-275.

Rahman, N. A. A., Sairi, I., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), 378-382.

Randol, B. M. (2014). Modelling the influence of organisational structure on crime analysis technology innovations in municipal police departments. *International Journal of Police Science & Management*, *16*(1), 52-64.

Ratner, C. (2021). When "sweetie" is not so sweet: Artificial intelligence and its implications for child pornography. *Family Court Review*, *59*(2), 386-401.

Raworth, K., Sweetman, C., Narayan, S., Rowlands, J., & Hopkins, A. (2012). *Conducting semi-structured interviews*. Oxfam

Renaud, P., Trottier, D., Rouleau, J. L., Goyette, M., Saumur, C., Boukhalfi, T., &

Bouchard, S. (2014). Using immersive virtual reality and anatomically correct computer-generated characters in the forensic assessment of deviant sexual preferences. *Virtual Reality*, *18*, 37-47.

Ray, K. N., & Miller, E. (2017). Strengthening stakeholder-engaged research and research on stakeholder engagement. *Journal of comparative effectiveness research*, *6*(4), 375-389.

Reyns, B. W., Henson, B., & Fisher, B. S. (2012). Stalking in the twilight zone: Extent of cyberstalking victimization and offending among college students. *Deviant behavior*, *33*(1), 1-25.

Richard Jr, M., & Unrau, Y. A. (2018). *Social work research and evaluation: Foundations of evidence-based practice*. Oxford University Press.

Ridder, HG. (2017). The theory contribution of case study research designs. Bus Res 10, 281-305. https://doi.org/10.1007/s40685-017-0045-z

Rideout, V., & Fox, S. (2018). Digital health practices, social media use, and mental wellbeing among teens and young adults in the US.

Riger, S, & Sigurvinsdottir, R. (2016). Thematic analysis. *Handbook of methodological approaches to community-based research: Qualitative, quantitative, and mixed methods*, 33-41.

Riley, R. W. (1996). Revealing socially constructed knowledge through quasi-structured interviews and grounded theory analysis. *Journal of Travel & Tourism Marketing*, *5*(1-2), 21-40.

Ringenberg, T. R., Seigfried-Spellar, K. C., Rayz, J. M., & Rogers, M. K. (2022). A scoping review of child grooming strategies: pre-and post-internet: Child Abuse & Neglect, 123, 105392.

Roberts, R. E. (2020). Qualitative Interview Questions: Guidance for Novice Researchers. *Qualitative Report*, *25*(9).

Rogers, M. (2003). Computer Forensics: Science or fad. *Secure Wire Digest* July 24, 2003b; 5 (55).

Rossler, M. T. (2019). The impact of police technology adoption on social control, police accountability, and police legitimacy. In *Political authority, social control and public policy*. Emerald Publishing Limited.

Rowe, M. (2020) Policing the Police: Challenges of democracy and accountability. In: Policing the Police: Challenges of democracy and accountability. Key Themes in Policing. Policy Press, Bristol. ISBN 9781447347057, 9781447348009, 9781447347064

Rowley, J. (2014). Designing and using research questionnaires. *Management research review, 37*(3), 308-330.

Ruggiano, N., & Perry, T. E. (2019). Conducting secondary analysis of qualitative data: Should we, can we, and how? *Qualitative Social Work, 18*(1), 81-97.

Russell, C. (1999). Interviewing vulnerable old people: Ethical and methodological implications of imagining our subjects. *Journal of aging studies, 13*(4), 403-417.

Rutkin, A. (2016). Could sex robots and virtual reality treat paedophilia? New Scientist. P 322, Broadhurst, R. (2019). *Child Sex Abuse Images and Exploitation Materials, in Roger Leukfeldt & Thomas Holt, Eds. Cybercrime: the human factor, Routledge.* 

Ryan L, Golden A (2006) Tick the box please': a reflexive approach to doing quantitative social research. *Sociology*. 40, 6,1191-1120.

Ryan, E., & Otonichar, J. (2016). Juvenile Sex Offenders. *Current Psychiatry Reports*, 18(7), 1-10.

Ryan, G.(2018). Introduction to positivism, interpretivism and critical theory. *Nurse Researcher*, 25(4) pp. 41–49

Sajithra, K., & Patil, R. (2013). Social media–history and components. *Journal of Business and Management*, 7(1), 69-74.

Saldaña, J. (2021). Coding techniques for quantitative and mixed data. *The Routledge Reviewer's Guide to Mixed Methods Analysis*, 151-160.

Salter, M., & Hanson, E. (2021). "I need you all to understand how pervasive this issue is": User efforts to regulate child sexual offending on social media, in *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*. Emerald Publishing Limited.

Sandhu, A., & Fussey, P. (2021). The 'uberization of policing'? How police negotiate and operationalise predictive policing technology. *Policing and Society, 31*(1), 66-81.

Santa Maria, A., Wolter, C., Gusy, B., Kleiber, D., & Renneberg, B. (2021). Reducing work-related burnout among police officers: The impact of job rewards and health-oriented leadership. *The Police Journal*, *94*(3), 406–

421. https://doi.org/10.1177/0032258X20946805

Saramago, M. A., Cardoso, J., & Leal, I. (2020). Victim crossover index offending patterns and predictors in a Portuguese sample. *Sexual Abuse*, 32(1), 101–124. https://doi.org/10.1177/1079063218800472

Sausdal, D. (2018). Everyday deficiencies of police surveillance: A quotidian approach to surveillance studies. *Policing and society*.

Scapens, R. W. (2004). Doing case study research. In The real life guide to accounting research (pp. 257-279). Elsevier.

Schaefer Morabito, M. (2010). Understanding community policing as an innovation: Patterns of adoption. *Crime & Delinquency*, *56*(4), 564-587.

Schaible, L.M., & Six, M. (2016). Emotional strategies of police and their varying consequences for burnout. *Police Quarterly*, 19 (1), 3-31.

Schmid, A. P. (2004). Frameworks for conceptualising terrorism. *Terrorism and political violence*, *16*(2), 197-221.

Schneider, G. P., & Evans, J. (2012). *New perspectives on the Internet: Comprehensive*. Cengage Learning.

Schreuders, Z.C., Cockcroft, T., Butterfield, E., Elliot, J., Soobhany, A.R., & Shan- A- Khuda, M. (2020). Needs Assessment of Cybercrime and Digital Evidence in a UK Police Force. *International Journal of Cyber Criminology*-ISSN: 0974-2891 January-June 2020.Vol.14 (1): 316-340.DOI: 10.5281/zendo.3757271

Schutz, A. (1962). The problem of social reality. In *Collected Papers: Volume IV* (pp. 71-72). Dordrecht: Springer Netherlands.

Schwartz, B. K. (2011). Characteristics and typologies of sex offenders. In B. K. Schwartz (Ed.), *Handbook of sex offender treatment* (pp. 1–33). Civic Research Institute.

Schwartz, J. (1993). Caution: Children at Play on the Information Highway. *The Washington Post*, *28*, A01.

Science Museum (2018). A computer in your pocket. The rise of smartphones. (Online). Retrieved on April 4, 2023, from: https://www.sciencemuseum.org.uk/.../computer-y

Scrivens, R., Windisch, S., & Simi, P. (2020). Former extremists in radicalization and counter-radicalization research. In *Radicalization and Counter-Radicalization*. Emerald Publishing Limited.

Seba, I., & Rowley, J. (2010). Knowledge management in UK police forces. *Journal of knowledge management*.

Seers, K. (2012). Qualitative data analysis. *Evidence-based nursing*, 15(1), 2-2.

Segre, S. (2014). A note on Max Weber's reception on the part of symbolic interactionism and its theoretical consequences. *The American Sociologist*, *45*, 474-482.

Seigfried-Spellar, K. & Leshney, S. (2016). The Intersection between social media, crime and digital forensics. *Digital Forensics. Threatscape and Best Practices, 2016, Pages 59-67.* 

Seigfried-Spellar, K.C., Soldino, V. (2020). Child Sexual Exploitation: Introduction to a Global Problem. In: Holt, T., Bossler, A. (eds) The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave Macmillan, Cham. <a href="https://doi.org/10.1007/978-3-319-78440-3">https://doi.org/10.1007/978-3-319-78440-3</a> 53

Senjo, S.R. (2004). An Analysis of Computer-Related Crime: Comparing Police Officer Perceptions with Empirical Data. *Security Journal*, 17: 55-71.

Seto, M. C. (2008). *Pedophilia and sexual offending against children: Theory, assessment, and intervention*. American Psychological Association.

Seto, M. C. (2017). The puzzle of male chronophilias. *Archives of Sexual Behavior*, *46*(1), 3-22.

Seto, M. C. (2019). The motivation-facilitation model of sexual offending. *Sexual Abuse*, *31*(1), 3-24.

Seto, M. C., Cantor, J. M., & Blanchard, R. (2006). Child pornography offences are a valid diagnostic indicator of paedophilia. *Journal of Abnormal Psychology*, *115*, 610–615. doi:10.1037/0021-843X.115.3.610.

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

Seto, M. C., Reeves, L., & Jung, S. (2010). Explanations given by child pornography offenders for their crimes. *Journal of sexual aggression*, *16*(2), 169-180.

Seto, M. C., Roche, K., Stroebel, M., Gonzalez-Pons, K., & Goharian, A. (2023). Sending, receiving, and nonconsensually sharing nude or near-nude images by youth. *Journal of Adolescence*.

Seto, M.C., Hanson, R.K., & Babchishin, K.M. (2011). Contact sexual offending by men with online sexual offences. *Sexual Abuse: A Journal of Research and Treatment*, 23 124-145

Shaffer, D. W., & Ruis, A. R. (2021). How we code. In *Advances in Quantitative Ethnography: Second International Conference, ICQE 2020, Malibu, CA, USA, February 1-3, 2021, Proceedings 2* (pp. 62-77). Springer International Publishing.

Sharif Razavian, A., Azizpour, H., Sullivan, J., & Carlsson, S. (2014). CNN features off-the-shelf: an astounding baseline for recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition workshops* (pp. 806-813).

Sharrock, W., & Button, G. (1991). The social actor: Social action in real-time. *Ethnomethodology and the human sciences*, *137*, 175.

Shaw, J. A., & Antia, D. K. (2010). Sexually aggressive youth. In E. P. Benedek, P. Ash, & C. L. Scott (Eds.), *Principles and practice of child and adolescent forensic mental health* (pp. 389–401). American Psychiatric Publishing, Inc.

Shawar, Y. R., Truong, P. P., & Shiffman, J. (2022). The emergence of political priority for addressing child sexual abuse in the United Kingdom. *Child Abuse & Neglect*, *128*, 105601.

Shell, B., Hung, M., Rueda, L. (2007). Cyber Child Pornography: A Review Paper of the Social and Legal Issues and Remedies- and a Proposed Technological Solution. *Aggression and Violent Behaviour* 12: 45-63.

Sherman, L. W. (1998). Ideas in American policing. Policing.

Sheth, J. (2020). Impact of Covid-19 on consumer behavior: Will the old habits return or die? *Journal of business research*, *117*, 280-283.

Shor, E. & Seida, k. (2019) "Harder and Harder"? Is Mainstream Pornography Becoming Increasingly Violent, and Do Viewers Prefer Violent Content? *The Journal of Sex Research,* 56:1, 16-28, DOI: 10.1080/00224499.2018.1451476

Siemens, G. (2005). Connectivism: A Learning Theory for the Digital Age. International *Journal of Instructional Technology and Distance Learning*. Vol. 2, No 1, pages 3-10

Singh, C. K., Pavithra, N., & Joshi, R. (2022). Internet an integral part of human life in 21st century: a review. *Current Journal of Applied Science and Technology, 41*(36), 12-18.

Simons, H. (2009). Case study research in practice. Case study research in practice, 1-200.

Sivesind, K. H. (1999). Structured, qualitative comparison. *Quality and Quantity, 33*, 361-380.

Sky News (2021). What is the Online Safety Bill, and why are some people worried about it? (Online) Retrieved on 14<sup>th</sup> March 2023 from: <a href="https://news.sky.com/story/what-is-the-online-safe">https://news.sky.com/story/what-is-the-online-safe</a>

Sloan III, J. J., & Paoline III, E. A. (2021). "They need more training!" A national level analysis of police academy basic training priorities. *Police Quarterly*, *24*(4), 486-518.

Sloper, P. (2004). Facilitators and barriers for coordinated multi-agency services. *Child: care, health and development, 30*(6), 571-580.

Smart Insights (2022). Global Social Media Research Statistics Summary, 2022. (Online). Retrieved on 24<sup>th</sup> August 2022, from <a href="https://www.smartinsights.com/social-media-mar-keting/social-media-strategy/new-global-social-media-keting/social-media-strategy/new-global-social-media-keting/social-media-strategy/new-global-social-media-

Smith, A. K., Ayanian, J. Z., Covinsky, K. E., Landon, B. E., McCarthy, E. P., Wee, C. C., & Steinman, M. A. (2011). Conducting high-value secondary dataset analysis: An introductory guide and resources. *Journal of general internal medicine*, *26*(8), 920-929.

Smith, E. (2008). *Using secondary data in educational and social research*. McGraw-Hill Education (UK).

Smith, J., & Noble, H. (2014). Bias in research. *Evidence-based nursing*, 17(4), 100-101.

Smithson, J. (2000). Using and analysing focus groups: limitations and possibilities. *International journal of social research methodology*, *3*(2), 103-119.

Snyder, H. N. (2000). *Sexual assault of young children as reported to law enforcement: Victim, incident, and offender characteristics. A NIBRS Statistical Report.* Washington, DC: Office of Justice Programs.

Spaapen, J., & van Drooge, L. (2011). Introducing "productive interactions" in social impact assessment. *Research Evaluation*, 20(3), 211–218

Specialist Child Abuse Investigator. (2023). College of Policing. (Online). Retrieved on 22<sup>nd</sup> February from <a href="https://profdev.college.police.uk/professional-profile/child-abuse-investigator">https://profdev.college.police.uk/professional-profile/child-abuse-investigator</a>

Spinello, R. A. (2000). Excerpt from cyberethics: morality and law in cyberspace. *Acm Sig-cas Computers and Society, 30*(1), 10-13.

Spohrer, J., Golinelli, G. M., Piciocchi, P., & Bassano, C. (2010). An integrated SS-VSA analysis of changing job roles. *Service Science*, *2*(1-2), 1-20.

Stake, R. E. (1995). *The art of case study research*. Sage.

Steel, C. (2021). Digital behaviours and cognitions of individuals convicted of online child pornography offences.

Steel, C. M. (2015). Web-based child pornography: The global impact of deterrence efforts and its consumption on mobile platforms. *Child abuse & neglect, 44,* 150-158.

Steel, C. M., Newman, E., O'Rourke, S., & Quayle, E. (2022). Improving child sexual exploitation material investigations: Recommendations based on a review of recent research findings. *The Police Journal*, 0032258X221142525.

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

Steel, C., Newman, E., O'Rourke, S., & Quayle, E. (2022). Technical behaviours of child sexual exploitation material offenders. *Journal of Digital Forensics, Security and Law, 17*(1), 2.

Steely, M., Ten Bensel, T., Bratton, T., & Lytle, R. (2018). All part of the process? A qualitative examination of change in online child pornography behaviours. *Criminal justice studies, 31*(3), 279-296.

Steinberg, H., Mollborn, S., & Pace, J. (2023). "Mature Enough to Handle it?": Gendered Parental Interventions in and Adolescents' Reactions to Technology Use During the Pandemic. *Journal of Family Issues*, 0192513X221150979.

Stewart, D. W., & Kamins, M. A. (1993). *Secondary research: Information sources and methods* (Vol. 4). Sage.

Stockdale, S. L., & Brockett, R. G. (2011). Development of the PRO-SDLS: A measure of self-direction in learning based on the personal responsibility orientation model. *Adult Education Quarterly*, *61*(2), 161-180.

Stratton, S. J. (2021). Population research: convenience sampling strategies. *Prehospital* and disaster Medicine, *36*(4), 373-374.

Stuart H. Suicidality among police. *Current Opinion in Psychiatry.* 2008 Sep;21(5):505-9. DOI: 10.1097/YCO.0b013e328305e4c1. PMID: 18650696.

Subrahmanyam, K., Smahel, D., Subrahmanyam, K., & Šmahel, D. (2011). Connecting online behavior to adolescent development: A theoretical framework. *Digital youth: The role of media in development*, 27-39.

Sullivan, J., & Quayle, E. (2012). Manipulation styles of abusers who work with children. *Creating safer organisations: Practical steps to prevent the abuse of children by those working with them*, 85-98.

Sunderji, N., & Waddell, A. E. (2018). Mixed methods convergent study designs in health professions education research: toward meaningful integration of qualitative and quantitative data. *Academic Medicine*, *93*(7), 1093.

Szegedy, C., Liu, W., Jia, Y., Sermanet, P., Reed, S., Anguelov, D., & Rabinovich, A. (2015). Going deeper with convolutions, in the proceedings of the. In *IEEE Conference on Computer Vision and Pattern Recognition* (pp. 7-12).

Taherdoost, H. (2018). A review of technology acceptance and adoption models and theories. *Procedia manufacturing*, *22*, 960-967.

Takahashi, D. (2016). Naughty America tries to get VR porn just right. Broadhurst, R. (2019). Child sex abuse images and exploitation materials. *Roderic Broadhurst, Child Sex Abuse Images and Exploitation Materials, in Roger Leukfeldt & Thomas Holt, Eds. Cybercrime: the human factor, Routledge.* 

Tashakkori, A., & Creswell, J. W. (2007). Exploring the nature of research questions in mixed methods research. *Journal of mixed methods research*, *1*(3), 207-211.

Tashakkori, A., & Teddlie, C. (1998). *Mixed methodology: Combining qualitative and quantitative approaches* (Vol. 46). sage.

Tashakkori, A., & Teddlie, C. (2010). Overview of contemporary issues in mixed methods. In A. Tashakkori & C. Teddlie (Eds.), *Handbook of mixed methods in social and behavioral research* (2nd ed.). Thousand Oaks, CA: Sage.

Teddlie, C., & Tashakkori, A. (2009). *Foundations of mixed methods research: Integrating quantitative and qualitative approaches in the social and behavioral sciences.* Sage.

Tehrani, N. (2018). Psychological well-being and workability in child abuse investigators. *Occupational medicine*, *68*(3), 165-170.

Tener, D., Wolak, J., & Finkelhor, D. (2015). A typology of offenders who use online communications to commit sex crimes against minors. *Journal of Aggression, Maltreatment & Trauma, 24*(3), 319-337.

Terry K. J. (2006). Sexual offenses and offenders: *Theory, practice and policy.* Wadsworth, Belmont, CA.

The Association of Police Crime Commissioners (2024). (Online). Retrieved on 1st August 2024 from <a href="https://apccs.police.uk/">https://apccs.police.uk/</a>

The Child Rescue Coalition (2020). Child Protection System. (Online). Retrieved on 15<sup>th</sup> March 2022 from <a href="https://childrescuecoalition.org/law-enforcement/">https://childrescuecoalition.org/law-enforcement/</a>

The Guardian (2022). Most convicted terrorists are radicalised online. (Online). Retrieved on 3<sup>rd</sup> March 2023 from: <a href="https://www.theguardian.com/uk-news/2022/dec/08/most-convicted">https://www.theguardian.com/uk-news/2022/dec/08/most-convicted</a>

The Guardian (2023). Covid lockdown created backdoor for child abusers, says charity. (Online). Retrieved on 8<sup>th</sup> April 2023 from <a href="https://www.theguardian.com/society/2023/jan/27/covid-lockdowns">https://www.theguardian.com/society/2023/jan/27/covid-lockdowns</a>.

The Internet: Independent Inquiry Child Sexual Abuse (2020). (Online). Retrieved on Jan 13, 2022, from <a href="https://www.iicsa.org.uk/">https://www.iicsa.org.uk/</a>

The National Crime Agency (2020). Online. Retrieved on 7 September 2021 from https://www.nationalcrimeagency.gov.uk/careers

The Open Rights Group (2020). Internet Watch Foundation. (Online). Retrieved on 7 October 2022 from: <a href="https://www.openrightsgroup.org/blog/informal-censorship-the-internet">https://www.openrightsgroup.org/blog/informal-censorship-the-internet</a>.

Police Federation (2022). Online. Retrieved on 1st August 2024 from <a href="https://www.polfed.org/">https://www.polfed.org/</a>

Thorne. (2016). The Intersection of child sexual exploitation and technology. (Online). Retrieved on 24<sup>th</sup> May 2022 from <a href="https://www.thorn.org/child-sexual-exploitation-and-technology/">https://www.thorn.org/child-sexual-exploitation-and-technology/</a>

Trott, M., Driscoll, R., Iraldo, E., & Pardhan, S. (2022). Changes and correlates of screen time in adults and children during the COVID-19 Pandemic: A systematic review and meta-analysis. *EClinicalMedicine*, 48.

Trottier, D., Goyette, M., Benbouriche, M., Renaud, P., Rouleau, J. L., & Bouchard, S. (2019). Using virtual reality with child sexual offenders: Assessing deviant sexual interests. *Virtual reality for psychological and neurocognitive interventions*, 209-225.

Tucker, W.T. (1965) Max Weber's Verstehen, The Sociological Quarterly, 6:2, 157-165, DOI: 10.1111/j.1533-8525.1965.tb01649.x

Twenge, J. M. (2017). Have smartphones destroyed a generation? *The Atlantic, 9*, 2017.

Twenge, J. M., & Martin, G. N. (2020). Gender differences in associations between digital media use and psychological well-being: Evidence from three large datasets. *Journal of adolescence*, *79*, 91-102.

Twenge, J. M., Haidt, J., Joiner, T. E., & Campbell, W. K. (2020). Underestimating digital media harm. *Nature Human Behaviour*, *4*(4), 346-348.

Tzanetakis, M. (2018). Comparing cryptomarkets for drugs. A characterisation of sellers and buyers over time. *International Journal of Drug Policy*, *56*, 176-186.

UK Safer Internet Center (2020). Self-generated Content. (Online). Retrieved on Jan 21, 2022, from <a href="https://saferinternet.org.uk/blog/tag/self-generated-content">https://saferinternet.org.uk/blog/tag/self-generated-content</a>

UK Safer Internet Safety (2020). New National Inquiry Into Disturbing Rise of Self-Generated Child Sexual Abuse Material. (Online) accessed on 19<sup>th</sup> March 2023 from <a href="https://www.saferinternet.org.uk/blog/new-national-">https://www.saferinternet.org.uk/blog/new-national-</a>

UK.GOV (2022). Characteristics of children in need. (Online). Retrieved on 27<sup>th</sup> April 2023 from: <a href="https://explore-education-statistics.service.gov.uk/find-statistics/characteristics-of-children-in-need">https://explore-education-statistics.service.gov.uk/find-statistics/characteristics-of-children-in-need</a>

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management science*, *46*(2), 186-204.

Verton, D. (2003). Black ice: the invisible threat of cyber-terrorism. Osborne.

Vijver, C. D. Van Der, & En Terpstra, J. B. (2007). 'Organisatie en sturing van politiewerk' [Organization of police work] in Fijnaut, C.J.C.F.

Violanti, J.M., & Gehrke, A. (2004). "Police trauma encounters precursors of compassion fatigue". *International Journal of Emergency Mental Health*, Vol. 6 No2, pp75-80

Vishnevsky, T., & Beanlands, H. (2004). Qualitative research. *Nephrology Nursing Journal*, *31*(2), 234.

Vito, G. and Higgins, G. (2010). 'Examining the validity of the leadership challenge inventory: The case for law enforcement.' *International Journal of Police Science and Management* 12(3): 305–319.

Vitorino, P., Avila, S., Perez, M., & Rocha, A. (2018). Leveraging deep neural networks to fight child pornography in the age of social media. *Journal of Visual Communication and Image Representation*, *50*, 303-313.

Vogels, E. A., & Sullivan, L. F. (2019). The relationship among online sexually explicit material exposure to, desire for, and participate in rough sex. *Archives of Sexual Behavior*, 48, 653–665. <a href="https://doi.org/10.1007/s10508-018-1290-8">https://doi.org/10.1007/s10508-018-1290-8</a>

Vogt, W. P., Vogt, E. R., Gardner, D. C., & Haeffeke, L. M. (2014). Selecting the Right Analyses for Your Data: Quantitative, Qualitative, and Mixed Methods; Guilford: New York, NY, USA. *Google Scholar*:

Von Behr, I. (2013). Radicalisation in the digital era: The use of the internet in 15 cases of terrorism and extremism.

Walden, I. (2013). Computer forensics and the presentation of evidence in criminal cases. In *Handbook of internet crime* (pp. 621-648).

Wall, D. (2007). *Cybercrime: The transformation of crime in the information age* (Vol. 4). Polity.

Wall, D. S. (2001). Cybercrimes and the Internet. Crime and the Internet, 1-17.

Walley, P., & Jennison-Phillips, A. (2020). A Study of Non-Urgent Demand to Identify Opportunities for Demand Reduction, *Policing: A Journal of Policy and Practice*, Volume 14, Issue 2, June 2020, Pages 542–554, https://doi.org/10.1093/police/pay034

Walsh, W. A., & Wolak, J. (2005). Nonforcible internet-related sex crimes with adolescents' victims: Prosecution issues and outcomes. *Child Maltreatment*, 10, 260-271

Warner, K., & Bartels, L. (2015). Juvenile sex offending: Its prevalence and the criminal justice response. *University of New South Wales Law Journal, The, 38*(1), 48-75.

Watkins, D. C. (2022). Secondary data in mixed methods research. SAGE Publications.

Watkins, D., & Gioia, D. (2015). *Mixed methods research*. Pocket Guide to Social Work Re.

Watkins, D.C. (2017). *Mixed methods research in social work.* Encyclopedia of Social Work Online. New York, NY: Oxford University Press.

Weatheritt, M. (Ed.). (2023). *Police Research: some future prospects*. Taylor & Francis.

Webb, L., Craissati & Keen, S. (2007). Characteristics of Internet Child Pornography Offenders: A Comparison with Child Molesters. *Sex Abuse (2007) 19.449-465* 

Weber, M. (1947). The theory of economic and social organization. *Trans. AM Henderson and Talcott Parsons. New York: Oxford University Press*.

Webster, H. J. (2014). Perceived stress among police officers: An Integrative model of stress and coping. *Policing: an International Journal of Police Strategies & Management*, 37 (4), 839-857

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

Weinman, G. (2004). *How modern terrorism uses the internet—United States Institute of Peace* (No. 116). Special Report.

Weisburd, D., & Lum, C. (2005). The diffusion of computerized crime mapping in policing: Linking research and practice. *Police practice and research*, *6*(5), 419-434.

Welsh, B. C., Braga, A. A., & Sullivan, C. J. (2014). The emerging link between public health and criminology is serious youth violence and innovative prevention. *Justice quarterly*, *31*(3), 500-523.

Werling, A. M., Walitza, S., Grünblatt, E., & Drechsler, R. (2021). Media use before, during and after COVID-19 lockdown according to parents in a clinically referred sample in child and adolescent psychiatry: Results of an online survey in Switzerland. *Comprehensive Psychiatry*, *109*, 152260.

Westera, N. J., Kebbell, M. R., Milne, B., & Green, T. (2016). The prospective detective: developing the effective detective of the future. *Policing and Society, 26*(2), 197-209.

Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review*, 9 (11), 39–52.

Westlake, B., Bouchard, M., & Frank, R. (2017). Assessing the validity of automated web crawlers as data collection tools to investigate online child sexual exploitation. *Sexual Abuse*, *29*(7), 685-708.

Weulen Kranenbarg, M. (2019). Contrasting cyber-dependent and traditional offenders: A comparison on criminological explanations and potential prevention methods. *Routledge Studies in Crime and Society*.

Williams, M., Butler, M., Jurek-Loughrey, A., & Sezer, S. (2021). Offensive communications: Exploring the challenges involved in policing social media. *Contemporary Social Science*, *16*(2), 227-240.

Wilson, C. (2003). Computer attack and cyber terrorism: vulnerabilities and policy issues for congress. *Focus on Terrorism*, *9*(1), 1-42.

Wilson, J. M., Grammich, C. A., Cherry, T., & Gibson, A. (2023). Police Retention: A Systematic Review of the Research. *Policing: A Journal of Policy and Practice, 17*, paac117.

Wilson, T. (2020). Collaborative Justice and Harm Reduction in Cyberspace: Policing Indecent Child Images. *The Journal of Criminal Law 2020*, Vol 84(5) 474-496:DOI: 10.117/0022018320952560

Wilson-Kovacs, D. (2021). Digital media investigators: challenges and opportunities in the use of digital forensics in police investigations in England and Wales. *Policing: An International Journal*, *44*(4), 669-682.

Wilson-Kovacs, D., Rappert, B., & Redfern, L. (2022). Dirty Work? Policing Online Indecency in Digital Forensics. *The British Journal of Criminology, 62*(1), 106-123.

Winter, C., Neumann, P., Meleagrou-Hitchens, A., Ranstorp, M., Vidino, L., & Fürst, J. (2020). Online extremism: Research trends in internet activism, radicalization, and counterstrategies. *International Journal of Conflict and Violence (IJCV)*, *14*, 1-20.

Winters, G. M., & Jeglic, E. L. (2022). Online Sexual Grooming. In *Sexual Grooming: Integrating Research, Practice, Prevention, and Policy* (pp. 65-86). Cham: Springer International Publishing.

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

Wolak, J. (2015). Technology-facilitated organized abuse: An examination of law enforcement arrest cases. *International Journal for Crime, Justice and Social Democracy, 4*(2), 18-33.

Wolak, J., Finkelhor, D., & Mitchell, K. (2011). Child pornography possessors: Trends in offender and case characteristics. *Sexual Abuse*, *23*(1), 22-42.

Wolak, J., Finkelhor, D., & Mitchell, K.J. (2009). Trends in arrests of 'online predators' (pp. 1–10). Durham: Crimes against Children Research Center, University of New Hampshire.

Wolak, J., Finkelhor, D., & Mitchell, K. (2011). Child pornography possessors: Trends in offender and case characteristics. *Sexual Abuse*, *23*(1), 22-42.

Wood, J. L., Alleyne, E., Ó Ciardha, C., & Gannon, T. A. (2020). An evaluation of polygraph testing by police to manage individuals convicted or suspected of sexual offending. The University of Kent <a href="http://kent.ac.uk/school-of-psychology/downloads/kent\_poly-graph\_report.pdf">http://kent.ac.uk/school-of-psychology/downloads/kent\_poly-graph\_report.pdf</a>

Woodbridge, J., Anderson, H. S., Ahuja, A., & Grant, D. (2018, May). Detecting homoglyph attacks with a Siamese neural network. In *2018 IEEE Security and Privacy Workshops* (*SPW*) (pp. 22-28)

Wright R, Powell M, Ridge D. (2006). Child abuse investigation: an in-depth analysis of how police officers perceive and cope with daily work challenges. *Policing: An International Journal of Police Strategies and Management*;29(3):498–512.

Wright, J. E., & Headley, A. M. (2021). Can technology work for policing? Citizen perceptions of police-body worn cameras. *The American Review of Public Administration*, *51*(1), 17-27.

Yannikos, Y., Schäfer, A., & Steinebach, M. (2018, August). Monitoring product sales in darknet shops. In *Proceedings of the 13th International Conference on Availability, Reliability and Security* (pp. 1-7).

Yar, M (2013). The Policing of the Internet sex offences: Pluraised sex offence governance versus hierarchies of standing. *Policing and Society.* 23:4, 482497 DOI: 10.1080/10439463.2013.780226

Yar, M., & Steinmetz, K. F. (2019). Cybercrime and society. Sage.

Yau, J. C., & Reich, S. M. (2019). "It's Just a Lot of Work": Adolescents' Self-Presentation Norms and Practices on Facebook and Instagram. Journal of Research on Adolescence, 29(1), 196–209. <a href="https://doi.org/10.1111/jora.12376">https://doi.org/10.1111/jora.12376</a>

Ybarra, M. L., & Mitchell, K. J. (2008). How risky are social networking sites? A comparison of places online where youth sexual solicitation and harassment occurs. *Pediatrics*, *121*(2), e350-e357.

Yin, Robert K. (2014). Case study research: Design and methods. Los Angeles, CA: Sage. Zakon, R. (1997). *Hobbes' Internet Timeline* (No. rfc2235).

Zeiger, S., & Gyte, J. (2020). *Prevention of Radicalization on Social Media and the Internet*. International Centre for Counter-Terrorism (ICCT).

Zhen, R., Li, L., Li, G., & Zhou, X. (2021). Social isolation, loneliness, and mobile phone dependence among adolescents during the COVID-19 pandemic: roles of parent–child communication patterns. *International Journal of Mental Health and Addiction*, 1-15.

Zvi, L., & Bitton, M. S. (2021). Perceptions of victim and offender culpability in the non-consensual distribution of intimate images. *Psychology, crime & law, 27*(5), 427-442.

# Appendix A: FOI Request, The Metropolitan Police

Information Rights Unit PO Box 313 Sidcup DA15 0HH United Kingdom

Web: www.met.police.uk

Email: MPSDataOffice@met.police.uk

Our Ref: 01/FOI/22/027327

Date: 22 December 2022

Dear Mr Harmson,

## FREEDOM OF INFORMATION REQUEST REFERENCE NO: 01FOI/22/027327

Thank you for your request for information which was received by the Metropolitan Police Service (MPS) on 14 November 2022, seeking access to the following information:

Do police officers and staff trained in grading indecent images of children hold formal or national accreditation for this role, similar to staff from the NCA and The Internet Watch Foundation?

#### **DECISION**

I have today decided to provide the data requested below.

#### **DISCLOSURE**

The MPS has a number of trainers who are formally trained and accredited by the Home Office. These trainers are then sanctioned to train other officers. However, those who receive the secondary training are not accredited in the same way as those trained by the Home Office.

This concludes your request for information and I would like to thank you for your interest in the MPS.

Should you have any further enquiries concerning this matter, please contact foia@met.police.uk, quoting the reference number listed.

Appendix B: FOI Request, West Yorkshire Police

Freedom Of Information PO BOX 9 Laburnum Road Wakefield WF1 3QP Tel: 01924 296006

Fax: 01924 292726 Email: foi@westyorkshire.police.uk Website: www.westyorkshire.po-

lice.uk

Our ref: FOI 1414950/22 Date: 09/12/2022 Dear Sir/Madam, Thank you for your request for

information, received by West Yorkshire Police on 14/11/2022. You requested the following

information:

Please inform me if police officers working within WYP, trained in the grading of indecent

images of children, hold any formal, recognised or national accreditation similar to staff from

the NCA or the Internet Watch Foundation. If they do hold any formal accreditation, what is

this called or known as? This information is part of my study into online sexual crimes inves-

tigation.

All Indecent Images of Children that are graded within West Yorkshire Police are done by Po-

lice Staff employees who are employed within the Digital Forensic Unit. All our trainers go on

the Grading of Child Sexual Abuse Material course held at the College of Policing which allows

for them to train our staff. The are classed as National Accredited Grading Trainers. They then

deliver the course called Grading of Child Sexual Abuse Material to our staff which makes

them Nationally Accredited Graders. COMPLAINT RIGHTS If you are not satisfied with how

this request has been handled or with the information provided, please read the advice notice

attached to this letter. If you do wish to take up your right of complaint, please remember to

quote the reference number above in any future correspondence.

Yours sincerely, XXXX Data & Information Sharing Officer

321

# Appendix C: FOI Request, West Midlands Police

Dear Mr Harmson

FOI Request Reference: 1544A/22

Thank you for your request for information, received on 14 November 2022.

#### **REQUEST**

Do police officers and staff who are trained in the grading of indecent images of children hold any formal or national accreditation or qualifications similar to staff from the NCA and The Internet Watch Foundation, who also grade indecent images of children?

#### **RESPONSE**

All OCSET (Online Child Sexual Exploitation Team) staff undertake College of Policing ICIDP (Initial Crime Investigators Development Programme) and SCAIDP (Specialist Child Abuse Investigators Development Programme) training in order to gain detective accreditation. However, they may begin viewing images before their training is complete. Some officers have also completed training delivered by the NCA who have recognised them as a 'Nationally Recognised Grader of IloC (indecent images of children)'.

## **RIGHT OF APPEAL**

Your attention is drawn to your right to request a re-examination of your case under West Midlands Police review procedure, which can be found at:

http://foi.west-midlands.police.uk/reviews-and-appeals/

Please note that such an appeal must be received within 40 working days of the date of this correspondence. Any such request received after this time will only be considered at the discretion of the FOI Unit.

If you require any further information, then please do not hesitate to contact me.

Yours sincerely,

**David Notley** | Freedom of Information Officer Corporate Communications | West Midlands Police

Preventing crime, protecting the public and helping those in need.

If it's not 999, search WMP Online

# Appendix D: E-mail. Permission response for use of data, from the Internet Watch Foundation

Hi XXX

Thank you for the prompt reply. Would it be possible at some point to visit with your analyst department to gain some first-hand experience in how they capture the data and what methods they use? It would be very beneficial to my research if this could be arranged. Please let me know if this would be possible.

Kindest regards Mike

## Hi Michael,

Unfortunately, we receive numerous requests from graduates doing research into our line of work, and we do not have the resources to accommodate the requests, so we will have to say we wish you all the best with your research, but feel free to use our data from our annual reports.

# Kind regards

#### **XXXXX**

**Business Officer** 

+44 (0) 1223 20 30 30 bill@iwf.org.uk iwf.org.uk