Exploring Online Sexual Extortion in Scotland

Robbie George Reid

LLB (Hons), Dip PLP

Submitted in fulfilment of the requirements for the Degree of LL.M(Research)

School of Law

College of Social Sciences

University of Glasgow

October 2019

ABSTRACT

This thesis provides a comprehensive review of an emerging criminal phenomenon: online sexual extortion. The conduct is part of a growing category of criminal acts characterised by the use of technology to commit sexual offences. This research follows on from recent academic, media and political discussion on related issues such as the non-consensual distribution of intimate images and 'up-skirting'. However, unlike these wrongs, online sexual extortion has received little treatment, particularly from a Scottish perspective.

In examining this issue, the thesis begins by drawing on existing literature in formulating a definition of online sexual extortion, with a broad definition being advocated. In recognising that the conduct is highly differentiated, a typology of the conduct is presented by reference to cases reported in the media and discussed in the literature. The focus then turns to coverage of the problem in Scotland. This is done by providing a review of leading literature on both the law and wider issues in this area. Statistical data is then analysed in order to chart the scale of the problem in Scotland, with it being concluded that online sexual extortion represents a growing threat that requires intervention. The thesis proceeds by examining the nature of the harms. It is argued that a distinct range of harms are experienced by victims and that these harms are exacerbated by the use of technology. Building on this, the multiple ways in which the conduct may infringe a victim's sexual autonomy are discussed. It is proposed that the wrong must be characterised as a sexual offence and that there are important conceptual and practical consequences of doing this. Additional violations in terms of damage to privacy and reputation along with financial harm are also examined. It is concluded that these factors collectively contribute to online sexual extortion being treated as a distinct criminal wrong. In assessing how well existing laws capture these harms and the wrongs of online sexual extortion, an evaluation of the criminal law framework in Scotland is then undertaken. Although acknowledged that there exist a number of offences that a perpetrator may be prosecuted under, it is argued that the response is far from satisfactory. This thesis concludes that legislative intervention would fill a gap in the current criminal law response. This could be achieved by introducing a discrete offence aimed at capturing more serious instances of sexual extortion. This would have important benefits in terms of reflecting the severity of the wrongdoing, the broader pattern of control, and range of harms experienced. It would additionally help raise awareness and be more effective in respect of fair labelling. A suggestion as to what the key elements of such an offence should be is offered in the final section of the thesis.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

I would like to express my gratitude to the Clark Foundation for Legal Education for their generous financial support which has allowed me to undertake this research.

I would also like to thank the following:

Professor James Chalmers for his input and advice over the course of my research, for which I am extremely grateful

Andrew Orr for always being there for me

My mum and dad for their continuous support

DECLARATION

I declare that, except where explicit reference is made to the contribution of others, that this dissertation is the result of my own work and has not been submitted for any other degree at the University of Glasgow or any other institution.

Robbie Reid

LIST OF ABBREVIATIONS

2003 Act:	Sexual Offences Act 2003
2009 Act:	Sexual Offences (Scotland) Act 2009
IBSA:	Image-Based Sexual Abuse
NSA:	National Crime Agency
SLC:	Scottish Law Commission
TFSV:	Technology-Facilitated Sexual Violence

INTRODUCTION

As we continue to witness technological advancements,[1] more opportunities emerge for existing offences to be committed in previously unimaginable ways.[2] This has led to a growing body of research on two categories of criminal wrongdoing where technology is used to commit a sexual wrong: 'image-based sexual abuse' (IBSA) and 'technology-facilitated sexual violence' (TFSV).[3] This research seeks to draw on and add to this literature by considering an emerging species of conduct that while falling within the parameters of these areas, has received little academic attention: online sexual extortion. Although somewhat neglected in terms of research, this does not reflect the severity of this conduct. As will be demonstrated in the course of this thesis, this conduct has the potential to cause great harm and the effects on victims can be severe.

As can be inferred from the label given to this conduct, the root of the wrongdoing lies in the offence of extortion. Extortion (and its English law counterpart blackmail)[4] is regarded as a serious crime[5] and its origins can be traced back as far as institutional writers including Alison[6] and Hume.[7] While considerable research has been undertaken on extortion and blackmail,[8] much of this has wrangled with conceptual questions such as the rationales for these offences.[9] This literature is vast and extends beyond the scope of this research. What this research rather seeks to do is examine the *specific* wrongs involved in online sexual extortion. It represents an example of cyber-enabled crime,[10] where an existing offence is committed in a different way through the use of technology. As the conduct straddles distinct criminal law categories including sexual offences, dishonesty offences and cybercrime, this

[1] J Clough, *Principles of Cybercrime* (2015) 5.
[2] E.g. online fraud scams, webcam hacking, online grooming of children through social media and chat sites, and cyber-stalking and harassment. See *Home Affairs Select Committee: E-crime* (2013, 5th Report of the Home Affairs Select Committee) HC 70 at 4.
[3] A literature review is set out at 2.1.
[4] These offences are used interchangeably in the literature. However, important differences exist between the Scots law offence of extortion and English law offence of blackmail: see below at 3.2.1.
[5] The offence is triable on indictment and can carry a severe sentence. See also P Alldridge, "Attempted murder of the soul: blackmail, privacy and secrets" (1983) 13 OJLS 368 at 369.
[6] A Alison, *Principles of the Criminal Law of Scotland* (1832) 576-579.
[7] D Hume, *Commentaries on the Law of Scotland, Respecting Crimes* (1797) I, 439.
[8] J Herring, *Criminal Law: Text, Cases, and Materials*, 3rd edn (2008) 614.
[9] This has been termed the "blackmail paradox". For an overview of the vast literature here see D Ormerod and K Laird, *Smith and Hogan's Criminal Law*, 14th ed (2015) 1070-71.
[10] Or 'technology-facilitated' crime.

is a complex form of criminality. It is therefore vital that research is undertaken and that proposals can be put forward as to how this problem should be addressed.

This issue will be approached from a substantive criminal law perspective. The primary objectives are to consider the specific ways that the conduct (i) violates, and (ii) can be targeted by, the criminal law. However, this is a socio-legal issue that cannot be examined in a criminal law vacuum. As such, reference will be made throughout to surveys and studies into the nature and effects of the conduct, with these helping shape any criminal law response. Furthermore, although a number of civil law remedies are available to victims,[11] the civil law's role is beyond the scope of this research, which only considers the criminal law response.

This research begins by examining what is meant by online sexual extortion. This will be done by reference to terminology used in related literature and existing definitions that have been adopted. A working definition will be proposed, which will be relied upon in the rest of the thesis. The chapter will continue by exploring the different types of behaviour falling within its scope. The purpose here is to sketch a picture as to which specific acts may be captured by the label 'online sexual extortion'. While it cannot be claimed that this is exhaustive, it will nevertheless provide an overview of the most common examples of the conduct, being distilled from reported cases, surveys, and media reports.

The first aim of the second chapter is to map the problem in Scotland through an examination of the literature, and by reference to official crime statistics. This will shed light on such issues as awareness and responses to online sexual extortion, while also giving some indication as to its prevalence.

The focus will then turn to the harms. This section will attempt to answer two of the key research questions of this thesis: (i) what are the harms of online sexual extortion and (ii) how do these differ from those of traditional extortion? That the conduct is wrongful and capable of causing serious harm may appear obvious. However, identifying specific interests that this wrongdoing violates is more challenging. This chapter will address this problem by

[11] E.g. actions for defamation or breach of privacy. Similarly, regulation of websites and social media platforms is another area where the civil law may play a role.

firstly assessing the extent to which online sexual extortion differs from sexual extortion in an offline context. It will be argued that the presence of the 'online' element represents a very different form of criminality and that the nature of the harms differs significantly as a result. Building on this, each harm will be examined in turn to establish the different ways in which victims' rights may be infringed. This will be done by reference to sexual harm, damage to privacy and reputation, and financial harm.

The third chapter will focus on the operation of substantive criminal law and consider the options available when prosecuting online sexual extortion under Scots law. The key question driving the research in this chapter is this: how suitable is the legal response to the problem? In answering this, the research will examine not only which offences may capture relevant conduct, but also assess whether these are suitable responses which adequately address harms experienced by victims.

The final chapter will pull together the research by focusing on how the conduct should be addressed under Scots law. It will be argued that improvements must be made to reporting procedures to encourage victims to come forward and that, as is the case with other cybercrimes, jurisdiction represents a fundamental problem. It will then draw on the assessment of the current law presented in the third chapter and propose a legislative solution that could better protect victims of online sexual extortion. This will be aimed at more effectively capturing this wrongdoing, which is inadequately addressed by Scots criminal law at present.

1 DEFINING ONLINE SEXUAL EXTORTION

This chapter will lay down the foundations for this thesis by examining three interconnected issues. It will begin by considering the significance of terminology in the field of sexual wrongs committed online, setting out why this matters. Drawing on existing literature including academic articles and empirical studies, it will be argued that the range of terminology relating to online sexual extortion is problematic and obscures meaningful understanding of the conduct.

The second section will consider a central component of this thesis: what is meant by 'online sexual extortion'? It is proposed that this should be defined in broad terms and a working definition of this will be formulated for the purposes of this thesis.

The conduct itself will then be examined. A typology will be formed with the aim of identifying different species of conduct present in online sexual extortion cases. This will be supported by reference to case law from Scotland and other jurisdictions, as well as studies into victims' experiences. Setting this out will allow for a detailed consideration of the types of interests this conduct threatens later in the thesis.

1.1 Terminology

This chapter aims to address issues concerning terminology. This will be done by considering the significance of having clear and consistent terminology, and it will be argued that in the particular context of online sexual extortion there is a need for greater consistency in the language used.

The importance of terminology cannot be overstated: "words matter because they shape our understanding of the problem, and guide our solutions".[1] In an area where terminology is abundant this is particularly the case. A key conclusion of a Europol report into the online sexual extortion and coercion of children was the "lack of common language and

[1] Subgroup Against the Sexual Exploitation of Children, NGO Group for the Convention on the Rights of the Child, "Semantics or Substance? Towards a shared understanding of terminology referring to the sexual abuse and exploitation of children" (Jan 2005). Report available at: *www.ecpat.org/wp-content/uploads/legacy/Semantics%20or%20Substnce.pdf*

understanding of this phenomenon".[2] This can be attributed to the fact that online sexual extortion is not an offence in itself and, as such, "the word is a kind of prosecutorial slang for a class of obviously criminal conduct that does not in reality correspond neatly with any known criminal offence".[3] This can be seen in the variety of terms used to describe the conduct. These include 'sextortion', 'sexual extortion', 'sexual blackmail', 'webcam blackmail', 'webcam sex scam', 'sexual harassment' and 'dating scam'.[4] The use of these varying terms can cause confusion and lead to unhelpful assumptions being made about the nature of online sexual extortion. For example, terms such as 'webcam blackmail' and 'dating scam' denote certain modes of perpetration. While references to these terms in the media may be in cases where online sexual extortion has occurred, this label can end up being lost at the expense of these other terms, which may fail to capture the seriousness or nature of harms suffered by the victim. It is imperative that law enforcement agencies and public bodies are consistent in their discussion of online sexual extortion so they can work together in addressing it. To ensure consistency in this thesis, the term 'online sexual extortion' will be used rather than narrower terms, which may merely relate to one species of this broader category of conduct.

Inconsistent and conflicting terminology is not confined to online sexual extortion, but is an example of a wider, systemic problem with cybercrime. This is exemplified by the findings of an Australian government-commissioned report into TFSV, where the lack of consistent terminology in describing 'technology-enabled' crime was highlighted as a central issue.[5] This is supported by McGlynn and Rackley who argue in the field of IBSA that "terminology frame debates and options for legal redress, as well as playing a vital expressive role".[6] In the particular context of TFSV, it has been said that "existing terminology and the laws…do not adequately capture the scope, nature or intersection of

[2] Europol, European Cybercrime Centre, *Online sexual coercion and extortion as a form of crime affecting children - Law Enforcement Perspective* (May 2017) at 6. Available at: *https://www.europol.europa.eu/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf*

[3] B Wittes, C Poplin, Q Jurecic and C Spera, "Sextortion: cybersecurity, teenagers, and remote sexual assault" (Center for Technology Innovation at Brookings, 2016) at 10.

[4] Europol, *Online Sexual Coercion* (n.2) at 9

[5] N Bluett-Boyd, B Fileborn, A Quadara and S Moore, "The role of emerging communication technologies in experiences of sexual violence: a new legal frontier?" (Australian Institute of Family Studies Research Report No.23, 2013) at 3. Available at: *https://aifs.gov.au/publications/role-emerging-communication-technologies-experiences-sexual-violenc*

[6] C McGlynn and E Rackley, "Image-based sexual abuse" (2017) 37 OJLS 534 at 535

such harms"[7]. This may be because the terminology draws on stereotypical coverage of such conduct or fails to reflect the severity of the wrongs. Parallels can be drawn with 'revenge porn', with the term being popularly used in the wider media despite there being no such offence. Recently enacted legislation on this in Scotland refrains from using this term and instead provides a much more suitable label: the non-consensual disclosure of intimate photographs or films.[8] This is much more beneficial in terms of focusing discussion on the wrong.

Similarly, just as there were concerns that 'revenge porn' skewed debates on this conduct, focusing on the motive (revenge) and nature of the material (pornography),[9] similar fears have arisen in respect of online sexual extortion. One problem is that this term (or 'sextortion') places too great an emphasis on the extortion element. There is concern that the word 'extortion' is inextricably linked with the idea of demands backed by threats of violence for the receipt of money or property. This can be attributed primarily to the relationship between extortion and property under English law.[10] This is one reason why the Europol report uses the term 'coercion' as well as extortion[11] because the conduct "is not simple extortion by means of a threat of reputational damage".[12] However, given the breadth of extortion under Scots law, this is less of a concern here as there is no requirement for violence or financial gain.[13]

1.2 Defining Online Sexual Extortion

It is imperative that a clear definition of online sexual extortion is adopted. The primary reason is to achieve clarity in the law and in practice.[14] A lack of a clear definition can be seen as contributing to the neglect of the problem by law enforcement agencies, journalists and public bodies.[15]

---

[7] A Powell and N Henry, "Sexual violence in the digital age: the scope and limits of criminal law" (2016) 25 Social and Legal Studies 397 at 398
[8] Abusive Behaviour and Sexual Harm (Scotland) Act 2016 s.2.
[9] McGlynn & Rackley (n.6) at 536.
[10] Theft Act 1968 s.34(2).
[11] Europol, *Online sexual coercion* (n.2)
[12] B Wittes, C Poplin, Q Jurecic and C Spera, "Closing the sextortion sentencing gap: a legislative proposal" (Center for Technology Innovation at Brookings, 2016) at 7.
[13] See 3.2.1
[14] In the reform of sexual offences a key aim of the project was to make the law clear: Report on *Rape and Other Sexual Offences* (Scot Law Com No 209, 2007) para 1.24.
[15] Wittes et al (n.3) at 4.

With many types of criminal conduct its exact nature is apparent from how it is labelled. One would intuitively think this would be the case with online sexual extortion; however, this is not necessarily so. It can manifest itself in a number of forms and much of the activity takes place in secrecy. As a result, "it remains relatively undefined".[16]

1.2.1 Existing Definitions

What definitions exist at present? It will now be shown that a number of definitions have been adopted under the label of 'online sexual extortion', thereby hindering progress that can be made in addressing the problem. This section will consider both the merits and shortcomings of using what will be referred to as the 'narrow definition' and 'broad definition' of online sexual extortion, arguing in favour of the latter. The definition adopted in this thesis will be important in assessing the criminal law response to this conduct and proposing how it can best be addressed in Scotland.

To begin with, the label implies that there are three, obvious, discrete elements. Firstly, that the conduct in question must be committed online. Secondly, that there must be a sexual element. And thirdly, that it must involve extortion. The presence of each of these elements distinguishes this conduct from offences such as the non-consensual distribution of intimate images or extortion itself. As such, neither of these offences alone suitably encapsulate the conduct.

In certain contexts, discussion of online sexual extortion has been narrowly framed around cases where the demand is of a sexual nature. This encompasses situations where an individual is threatened into doing something sexual. The focus here is the demand of the perpetrator. Such a definition captures archetypical cases of 'webcam blackmail', where a victim is threatened into performing sexual acts on a webcam. It would also include situations where a victim is threatened into sending sexual images or material. The Europol report is consistent with this and defines the purpose as being to "obtain sexually explicit

[16] ibid at 9.

material or sexual favours".[17] This definition has been adopted in other works[18] and a Brookings Institute article similarly defines it as "old-fashioned extortion or blackmail, carried out over a computer network, involving some threat…if the victim does not engage in some form of further sexual activity".[19] In such instances the harm to the victim would not only be the potential violation of their sexual autonomy where they comply. The threat itself may pose a violation to their liberty, and additionally to their right to privacy, or reputation. Clearly this is a serious wrong; however, it will be argued that online sexual extortion extends beyond this specific conduct.

1.2.2 Proposing a Definition

Firstly, this narrow definition fails to cover cases where the demand is not sexual (e.g. it may be financial), but the threat is sexual. There is still a clear violation of an individual's sexual autonomy where a threat is made to further infringe their autonomy, regardless of whether this is by demands of a sexual nature, or financial demands.[20] In all these situations the conduct remains inherently sexual. Narrow definitions do not therefore adequately recognise differing modes of perpetration that exist among perpetrators.

Secondly, they fail to take account of changing motivations. While an individual may initially seek to watch the victim engaging in sexual activity or obtain sexual material, this may not be all they set out to do. They may then use this material to issue further demands to the victim (e.g. financial) with an accompanying threat to disseminate previously acquired content.[21] It is clear that such a threat is still a breach of a victim's sexual autonomy and should be included within the scope of online sexual extortion, regardless of the fact that the demand is no longer sexual. In recognising the varying demands and motivations of perpetrators of online sexual extortion, the Crimes Against Children Research Center's definition is preferable. By defining 'sextortion' more broadly as "threats to expose a sexual image in order to make a person do something or for other reasons, such as revenge or

[17] Europol, *Online sexual coercion* (n.2) at 15.
[18] E.g. Powell & Henry (n.7) at 407; B Wittes, "Cyber sextortion and international justice" (2017) 48 Georgetown Journal of International Law 941 at 942, 945.
[19] Wittes et al (n.3) at 11.
[20] See discussion of the sexual harms below at 2.5.1(a).
[21] D Lee, "Teenager's death sparks cyber-blackmailing probe", BBC News (16 Aug 2013). Available at: *http://www.bbc.co.uk/news/uk-scotland-edinburgh-east-fife-23712000*

humiliation"[22] they take account of sexual threats. However, the downsides of such a definition are, firstly, that threatening to expose a sexual image for revenge or humiliation is a separate criminal wrong that (assuming there is no demand) does not amount to extortion, and secondly, that it frames the threatening behaviour in terms of exposing a sexual image without appreciating other threats that may be employed. In the UK, even the NCA can be accused of skewing perceptions. While not providing a precise definition, they nevertheless describe it as conduct through which "criminals might befriend victims online by using a fake identity and then persuade them to perform sexual acts in front of their webcam".[23] This illustrative statement further misrepresents online sexual extortion by emphasising deception. Although this may be present in many cases, the description fails to capture different ways that an online relationship may begin and develop. It additionally does not take account of online sexual extortion in existing relationships and domestic abuse cases. In some instances the victim may be perfectly aware of the identity of the perpetrator (whether personally known to them or not) and in other cases the victim may be initially willing to perform sexual acts or send intimate images without coercion or deception. Discussion of this conduct in such narrow terms diverts attention from other common features and places too much attention on particular *modes* of perpetration.

In combatting these problems, a broader definition of online sexual extortion is adopted for the purposes of this thesis. This adequately covers the many forms that this conduct takes and is based on the following observations:

- that an individual's sexual autonomy may be violated in many ways;
- that the perpetrator's demand is not always sexual in nature; and
- that deception is a common element, but not essential.

Drawing on these considerations, online sexual extortion is defined as instances where an individual, A, engages in conduct facilitated by a technological device with another individual, B, and by means of a threat, demands that B acts in a way that is against their will, where either the threat or demand is sexual in nature.

[22] J Wolak and D Finkelhor, "Sextortion: findings from a survey of 1,631 victims" (Crimes Against Children Research Center, 2016) at 5. Available at: *https://www.wearethorn.org/wp-content/uploads/2016/08/Sextortion_Report.pdf*

[23] NCA information page on "Sextortion". Available at: *https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/kidnap-and-extortion/sextortion-webcam-blackmail*

This definition ensures that conduct is caught so long as either the threat or demand is sexual in nature and also provides that undue emphasis is not placed on one particular mode of perpetration.

1.3 Establishing a Typology of Conduct

In light of what is argued above, there is no consistent pattern of behaviour. Certain elements such as fraud and deception may be present in many, but not all, instances. In addition to this, continuous technological developments have resulted in a lack of empirical research illustrating the ways that technology facilitates sexual violence.[24] This further complicates the task of identifying species of conduct falling under the heading of online sexual extortion.

An attempt will nevertheless be made to break down different species of behaviour by reference to key features of online sexual extortion cases. This section will seek to examine the significance of each of these. It will begin by exploring the presence of consent and following this will examine the relevance of the parties' status, modes of facilitation, and lastly, the distinction between preparatory and substantive criminal conduct. As will be shown, there are important legal distinctions between the types of conduct discussed and, as such, this is a necessary exercise for the purposes of evaluating the criminal law response in Chapter 3.

1.3.1 Sexting and Non-Consensual Conduct

Firstly, it is important to distinguish online sexual extortion from sexting.[25] Although certain types of conduct may be considered risky[26] (e.g. sexting; consensual sharing of images), these behaviours on their own are unlikely to be criminal.[27] Sexting has been defined as "the consensual taking and consensual sharing of semi-nude/nude/explicit images

[24] Bluett-Boyd et al (n.5) at 4.
[25] E Quayle, "Over the Internet, under the radar: online child sex abuse and exploitation – a brief literature review" (2017) at 3; Wittes et al (n.3) at 3.
[26] In the sense that although they may initially involve the consensual sharing of intimate images or other media, this material may later be used in ways they had not consented to.
[27] Except where the sexting is between an adult and child or between two children.

with the intended recipient".[28] Thus, the difference between sexting and 'sextortion' is that sexting is typically consensual. The question of whether an individual therefore notionally consented to doing anything sexual will rarely be of significance in the case of the latter; consent will likely be negated by the perpetrator's threats.

However, that is not to say that consensual conduct such as sexting may never be relevant to online sexual extortion. It frequently features as a preliminary act in situations where the victim consensually sends images or other intimate material to an individual who plans, or later uses this material, to coerce the victim. Although this does not change the nature of the initial sending of material (which remains consensual), it represents a very different wrong.

Furthermore, as will be discussed in the next section, where one of the individuals participating in sexting is under the age of 16, then regardless of whether there is any factual consent, this will still be a criminal wrong, even prior to any coercive acts by the perpetrator.

1.3.2 Status of the Parties

Secondly, there are differences in the categorisation of the conduct depending on the status of the parties. The two main issues here relate, firstly, to the age of the parties, and secondly to their relationship. The nature and degree of criminality may vary according to the status of the parties involved.

In terms of age there are four possibilities:

(i) A and B are both adults

(ii) A is an adult and B is a child

(iii) A and B are both children

(iv) A is a child and B is an adult[29]

[28] Bluett-Boyd et al (n.5) at 2.

[29] Although no examples of a child engaging in online sexual extortion against an adult have been found in the course of this research, it is entirely conceivable that a 15 year old could sexually extort a 16 year old.

Age is a significant consideration. Where the victim is a child then the issue of consent differs. The Sexual Offences (Scotland) Act 2009 is modelled on the protective principle: that sexual activity by a person over the age of 16 with anyone under the age of 16 is criminal.[30] However, its approach differs depending on the child's age. Separate offences exist where the criminal conduct involves what the legislation terms as 'older' (a child who has attained the age of 16) and 'younger' (a child who has attained the age of 13 but not yet attained the age of 16) children. Where a 'younger child' is involved, the law does not have to engage with the task of showing that consent was absent. The legislation simply acknowledges that it is impossible for consent to be given in such circumstances. However, where the victim is an older child it will be necessary to consider consent, not in terms of assessing if there is criminal liability, but in determining the severity of the offence. The practical implication of this is that where factual consent is present, the correct offence with which the accused should be charged is that specifically relating to an older child.[31] Recognising this distinction allows for the conduct to be appropriately distinguished, resulting in a more focused approach to dealing with the conduct.

As well as age, whether a pre-existing relationship exists between the parties is relevant. There have been found to be "substantial differences in dynamics"[32] between this relationship, and one that develops online with a stranger. This has consequences both for the harms sustained by the victim, and also their ability to report wrongdoing. In terms of harm, perpetrators can exercise a greater degree of control over the victim within a pre-existing relationship. Research has found that in the majority of these cases, the primary motivation of the perpetrator is to demand or coerce the victim into returning or remaining in a relationship with them.[33] It is therefore important to recognise the specific harms that may be felt in these cases, as well as noting that such conduct may be part of a wider pattern of domestic abuse and result in liability for the recently introduced coercive control offence.[34]

[30] Report on *Rape and Other Sexual Offences* (n.14) para 1.28.
[31] *WD v McPherson* 2013 SCCR 305.
[32] Wolak & Finkelhor (n.22) at 8.
[33] ibid at 22.
[34] Domestic Abuse (Scotland) Act 2018 s.1; see 3.3.4.

1.3.3 Methods of Perpetration

Thirdly, it must be recognised that online sexual extortion covers a range of conduct and is "multivariate in character".[35] Can any patterns be identified?

It is suggested that the conduct may begin from three different factual bases.

These are:

(i) Where the perpetrator, A, by deception, establishes communication with the victim, B, through a website or online application.

(ii) Where the perpetrator, A, without using deception, establishes communication with the victim, B, through a website or online application.

(iii) Where the perpetrator, A, remotely gains access to either a computer, webcam or online account belonging to the victim, B.

Thus, the perpetrator will either initially engage with the victim by deception, without deception, or by remotely accessing a technological device or online account belonging to the victim. These modes of establishing contact with victims can be seen in reported cases from other jurisdictions and will now be considered. These not only have important consequences from a purely legal perspective - they may impact the offences with which the perpetrator can be charged - but also from a law enforcement perspective, with the response differing according to the mode of perpetration.

1.3.3(a) Deception

Given the ease with which perpetrators of online offences can deceive victims, it is unsurprising that deception features prominently in online sexual extortion cases. In a survey of young victims, 55% of respondents in their first interaction with a perpetrator claimed

[35] Wittes (n.18) at 943.

they were deceived or given a false impression as to their identity or features.[36] Lies and misrepresentations most commonly related to age, gender or the aggressor's intentions.[37] In some instances even the identities of the victims' partners were assumed as a means of deceiving victims.[38] Examples of such conduct can be seen in the cases discussed below.

In the recent English case of *R v Knight (Jordan)*[39] the defendant was convicted of causing or inciting a child to engage in sexual activity.[40] This involved deception as to the defendant's age by communicating with the victim over Facebook and telling her he was 18 years old, when he was in fact 20. However, deception has gone further than this. In two earlier English decisions victims were deceived by individuals personally known to the victim. In *R v Devonald*,[41] the father of the victim's former girlfriend posed as a young female before encouraging the victim to engage in sexual activity, footage of which was then used to extort him. Deception as to identity was also a means of coercing the victim in the subsequent case of *R v Bingham*,[42] where the defendant assumed multiple identities in order to exert control over the victim who was his girlfriend. The numerous means of deceiving unsuspecting victims allows individuals to target large numbers of people not previously known to them with little threat of them being identified and reported. In the Canadian case of *R v. Miller*[43] the defendant engaged in conversations with an estimated 300 girls,[44] frequently lying about his age and gender. The girls were coerced into performing sexual acts, sending intimate images, and providing details of other girls for the defendant to message. Where they failed to comply the defendant threatened to physically harm the victims or expose them to relatives or friends.

In the unreported Scottish case of *HM Advocate v McBride*[45] the offending was similar. False identities were used to develop relationships with victims. This extended to false social media accounts where victims were encouraged to connect with him. On doing this, McBride

[36] Wolak & Finkelhor (n.22) at 13.
[37] ibid.
[38] Wittes et al (n.3) at 2.
[39] [2017] EWCA Crim 1940.
[40] Sexual Offences Act 2003 s.10(1)
[41] [2008] EWCA Crim 527.
[42] [2013] EWCA Crim 823.
[43] 2011 ABPC 354.
[44] ibid at para 3.
[45] *HM Advocate v Andrew McBride*, sentencing statement published on Judiciary of Scotland website. Available at: http://www.scotland-judiciary.org.uk/8/1360/HMA-v-ANDREW-MCBRIDE

repeatedly threatened to distribute intimate images of the victims unless they complied with further demands.

Technology provides fertile conditions in which deception can be carried out without going to great lengths. Bogus social media accounts can be established by simply creating a false email address, which can be easily done without verifying your identity.[46] This allows for online sexual predators to establish multiple identities on web-based platforms, thus equipping them with a strong arsenal with which to carry out online sexual extortion.

While these examples illustrate the potential afforded to perpetrators when it comes to deceiving victims, deception extends beyond identity, and may concern the intentions of the perpetrator. This can be seen in the recent case of Matthew Falder, a serial online sexual predator who engaged in online sexual extortion over an eight year period. Falder sought out victims and obtained sexual images by posing as a female artist looking for life models online, and by posting on advertising sites such as Gumtree.[47] This is similar to where perpetrators pose as a legitimate person from a casting or modelling agency, or photography studio.[48] In these cases the material is obtained fraudulently and once the perpetrator possesses this they may extort victims for additional material, live sexual acts, physical contact, or money.

1.3.3(b) Absence of Deception

There are instances where the perpetrator uses other techniques in order to establish communication with victims. Although not mutually exclusive from deception, these means do not *require* deception. These include techniques such as using disinhibiting conduct, positive inducements, and building a rapport.

[46] J Clough, *Principles of Cybercrime*, 2nd edn (2015) 7. For a more detailed discussion of this see 2.4.2(a).
[47] "Matthew Falder posed as female artist for online sex attacks" BBC News (16 Oct 2017). Available at: *http://www.bbc.co.uk/news/uk-england-birmingham-41640079*
[48] Europol, *Internet Organised Crime Threat Assessment (IOCTA) Report* (2017) at 38. Available at: *https://www.europol.europa.eu/sites/default/files/documents/iocta2017.pdf*

1.3.3(b)(i) Disinhibiting Conduct

Perpetrators may target potential victims by using 'disinhibiting conduct'. An example of this is inciting individuals to look at child pornography in order to erode their vulnerability and then use this as a means of coercion by threatening to disclose this if they fail to comply.[49] There are similarities here with tactics used by those engaging in online grooming, harassment and cyberstalking. Thus, a common strategy (particularly where the victim is a child) appears to be making the victim believe that they themselves are engaging in illegal activity. This is not novel, with the threat to report someone of having committed a criminal offence being a long-established sub-category of blackmail and extortion.[50] However, technology has made this much easier and more opportunities exist to incite unsuspecting victims into committing offences. In responding to this, efforts have been made to make children aware they are not committing any crime where they are coerced online into carrying out acts against their wishes. From a Scottish perspective, Police Scotland have sought to increase awareness of this and reassure victims that they are not the ones in the wrong.[51]

1.3.3(b)(ii) Positive Inducements

Although online sexual extortion is frequently characterised by a demand backed by a threat, it is also possible that an individual may bribe the victim into satisfying their desires.[52] In these instances the perpetrator's demand will be accompanied by an inducement or promise to do something, rather than a threat. Such inducements may be financial in nature or even the promise of a job. On its own, a bare inducement which the victim acts upon will not be an example of online sexual extortion due to the absence of a threat. However, extortion may occur where the victim is induced by the bribe and the extorter uses what they

[49] R O'Connell, "From fixed to mobile Internet: the morphing of criminal activity online", in M Calder (ed), *Child Sex Abuse and the Internet: Tackling the New Frontier* (2004) 37 at 53.
[50] M Hepworth, *Blackmail* (1975) 15. The other sub-categories mentioned are blackmail through physical threats and blackmail by means of threats to broadcast any discreditable statement.
[51] Police Scotland, "Police Scotland advice to child victims of online extortion" (20 Sep 2013). Available at: *http://www.scotland.police.uk/whats-happening/news/2013/september/advice-to-child-victims-of-online-extortion/*
[52] A Barak, "Sexual harassment on the Internet" (2005) 23 Social Science Computer Review 77 at 80.

have obtained to coerce them. Such conduct could therefore feature as a prelude to online sexual extortion.

1.3.1(b)(iii) Building Rapport

Where a perpetrator does not resort to deception or remotely obtain private material relating to the victim, they may try to form a bond with the victim and to develop a rapport with them. Research into this conduct has found that by enabling prolonged communication between perpetrator and victim, the Internet has led to an acceleration in the building of trust between both individuals.[53] Additionally, rapport in itself may be achieved by use of positive inducements or disinhibiting conduct referred to above.

1.3.3(c) Remote Access

The final distinct mode of perpetration is remotely accessing victim's devices or online accounts (hacking). This enables a perpetrator to obtain personal information relating to the victim, or sexual material belonging to them. By doing this, the perpetrator has the potential to later carry out online sexual extortion.

How might a perpetrator do this? This may be done by webcam hacking where the perpetrator, by having control over the victim's webcam, is able to covertly watch and record the acts of the victim. In addition to doing this covertly, the perpetrator may be able to use material obtained thereby as a means of coercing the victim into performing sexual acts.

Extortion may also involve hijacking an online account, and failing to relinquish control until the victim complies with specified demands.[54] In the Canadian case of *R v Mackie*[55] the defendant accessed the complainant's Facebook profiles in order to coerce them into sending explicit images. This was done by promising to relinquish control of the account in return for more images.[56] This mode of hacking was used to carry out a sophisticated blackmail

[53] M G McGrath and E Case, "Forensic psychiatry and the Internet" (2002) 30 J Am Acad Psychiatry Law 81 at 87.
[54] *R v Mackie* 2013 ABPC 116 at para 4.
[55] ibid.
[56] ibid at para 4.

scheme in the English case of *R v Egege*[57] where the defendant hacked the victim's email account and set up fake social media accounts purporting to belong to the victim. They contacted the victim's relatives and friends using these accounts and subsequently threatened the victim with the exposure of intimate images and videos they had acquired unless they received £300.

Although remotely accessing another individual's technological device or online accounts may be a vehicle for online sexual extortion, it is on its own no more than this. In this context it can be better viewed as preparatory conduct. Like sexting, it may enable a perpetrator to later carry out extortion, but itself falls short of constituting online sexual extortion. It has been observed that "unwanted sexual attention in cyberspace usually necessitates direct personal verbal communication between a harasser and a victim"[58] and this is consistent with the definition provided in the previous chapter: that online sexual extortion will involve the presence of a demand backed by a threat, which requires communication with the victim.

1.3.4 Substantive vs Preparatory Conduct

Finally, it is important to consider the conduct itself. It has been shown that there are numerous different starting points for this conduct even before a single demand or threat is communicated. By separating different species of conduct out, it allows us to better consider legal responses to online sexual extortion.

In order to avoid conflation of these types of conduct, they have been separated into two groups: preparatory conduct and substantive conduct. This distinction will be drawn according to the definition of online sexual extortion set out above.

Preparatory conduct consists of conduct that may be present in online sexual extortion cases, but that on its own falls short of constituting online sexual extortion. This includes, among others, the following:

(i) Hacking and computer misuse

(ii) Fraud

[57] [2017] EWCA Crim 2161.
[58] Barak (n.52) at 80.

(iii) Indecent communication
(iv) Threatening behaviour
(v) Voyeurism
(vi) Sexual Exposure
(vii) Grooming
(viii) Pornography offences

Substantive conduct, on the other hand, is more characteristic in itself of online sexual extortion. This includes the following:

(i) Extortion
(ii) Causing the victim to engage in a sexual act
(iii) Causing the victim to be present during sexual activity

Clearly, suitable criminal responses to preparatory conduct are important in allowing the perpetration of criminal behaviour to be stopped and for intervention to occur at an earlier stage, prior to the commission of more serious conduct.

In summary, this chapter has identified problems with overlapping terminology and recommended the use of “online sexual extortion” as a suitable label for the conduct in question. While other definitions have been narrower in scope, this thesis has adopted a broader one in recognising varying sexual harms suffered by victims. Finally, the conduct was examined according to key features of the offending. It was proposed that the conduct may be categorised and distinguished according to the age of the parties, the existence of a relationship between them, the methods of establishing communication with victims and obtaining material with which to extort them, and the distinctions between preparatory and substantive conduct.

2 MAPPING THE PROBLEM OF ONLINE SEXUAL EXTORTION IN SCOTLAND

This chapter will seek to build on the work in the previous chapter by mapping the problem of online sexual extortion in Scotland. This will pave the way for a more detailed evaluation of the conduct in the rest of this thesis. This chapter has three clear aims. The first is to provide a review of the literature in the field. The second is to examine the presence of online sexual extortion as an issue in Scotland and to set out evidence as to its prevalence. The third is to identify and examine the wrongs of online sexual extortion. This will involve an examination of the different interests that are violated by the conduct. Only by mapping these harms can the existing criminal law framework be evaluated.

2.1 Literature Review

2.1.1 Literature on the Law

The legal literature on online sexual extortion in Scotland is underdeveloped. A survey of leading criminal law works has uncovered little to no mention of this conduct. Traditional criminal law textbooks focus more on substantive offences[1] and generally do not pay attention to different modes, or emerging types, of perpetration. This is particularly so where there is no discrete offence and where the conduct can be viewed as an amalgam of other offences. Criminal law works have nevertheless played an important role in this research when evaluating the legal framework, despite not offering much on the specific problem of online sexual extortion.

However, even in books dealing specifically with cybercrime, the issue receives little treatment.[2] Much research has focused on online extortion from a corporate perspective and

[1] G H Gordon, *Criminal Law of Scotland*: Vol 2, 4th edn, by J Chalmers and F Leverick (2016); D Ormerod and K Laird, *Smith and Hogan's Criminal Law*, 14th ed, (2015); A P Simester, J R Spencer, F Stark, G R Sullivan and G J Virgo, *Simester and Sullivan's Criminal Law: Theory and Doctrine*, 6th edn (2016).
[2] A Gillespie, *Cybercrime: Key Issues and Debates* (2015); J Clough, *Principles of Cybercrime*, 2nd edn (2015); D K Citron, *Hate Crimes in Cyberspace* (2014); D Wall (ed), *Crime and the Internet* (2001); P Grabosky, *Cybercrime* (2016); Y Jewkes (ed), *Crime Online* (2007); D Wall (ed), *Crime and Deviance in Cyberspace* (2009).

the growing trend of cybercriminals and hackers holding companies to ransom in return for payment.[3] This is an important issue[4] but when it comes to private victims "less attention has been paid to 'technology-facilitated sexual violence', where new technologies are used as tools to perpetrate or extend the harm of a sexual assault".[5]

Despite this, recently there has been a rapid growth of literature in this area, particularly from a feminist perspective. Several authors have been influential including Powell, Henry, McGlynn, Rackley, Hughton and Citron. In particular, much attention has been devoted to McGlynn and Rackley's conceptualisation of conduct as IBSA, and specifically the well-publicised issue of the non-consensual distribution of intimate images.[6] Much of these works have additionally considered grooming, 'up-skirting', and cyber-stalking, perhaps as a result of greater media and legislative attention. However, less focus has been paid to online sexual extortion,[7] which remains "remarkably understudied".[8] In the context of IBSA, neglect of other species of offending is acknowledged by McGlynn and Rackley, who state that "focussing the law and public debate too narrowly around classic 'revenge porn' cases is obscuring from public view, and legal redress, other forms of image-based sexual abuse".[9] Although online sexual extortion extends beyond IBSA,[10] this nevertheless shows that a change of focus would help in better tracking the scale of the conduct and in identifying appropriate legal responses to it. Broader than IBSA is TFSV,[11] a concept pioneered primarily by Powell and Henry. TFSV is "where mobile and online technologies are used as tools to blackmail, control, coerce, harass, humiliate, objectify or violate another person".[12] This category therefore comprises wrongs extending beyond the misuse of sexual images. As a result, online sexual extortion falls within this conceptualisation, despite a similar lack of attention being paid to it in terms of research output. One of the leading and most up-to-date works is Powell and Henry's *Sexual Violence in a Digital Age*.[13] This covers various

[3] See M D Griffiths, "Internet corporate blackmail: a growing problem" (2004) 168 Justice of the Peace 632-633; S Bremner, *Cybercrime: Criminal Threats from Cyberspace* (2010) 80-81; Wall, ibid 31-32.
[4] See Gillespie, *Cybercrime* (n.2) 41-42, where it is stated that hacking remains much more prevalent among corporations and governments than individuals.
[5] A Powell and N Henry, "Sexual violence in the digital age: the scope and limits of criminal law" (2016) 25 Social & Legal Studies 397 at 397.
[6] Colloquially referred to as 'revenge porn'.
[7] B Wittes, C Poplin, Q Jurecic and C Spera, "Sextortion: cybersecurity, teenagers, and remote sexual assault" (Center for Technology Innovation at Brookings, 2016) at 9.
[8] ibid at 6.
[9] C McGlynn and E Rackley, "Image-based sexual abuse: more than just 'revenge porn'" (2016) Research Spotlight Publication at 2.
[10] Although images may be used to extort further sexual material from victims or coerce them into engaging in sexual activity, they are not the only means of doing this.
[11] Powell & Henry (n.5) at 398.
[12] ibid.
[13] A Powell and N Henry, *Sexual Violence in a Digital Age* (2017).

types of TSFV (including a brief mention of 'sextortion')[14] but tackles these issues primarily from a feminist perspective and only deals with the experiences of adult victims. As a result, it does not engage with issues of substantive criminal law nor address the conceptual nature of online sexual extortion.

Moreover, framing debates regarding IBSA and TFSV solely in terms of gender and crimes against women is problematic. Although generally accepted that these are overwhelmingly crimes committed against women,[15] media reports and guidance from law enforcement bodies have suggested that a large number of men also fall victim to online sexual extortion.[16] One only needs to look at two of the Scottish examples discussed in this thesis to see that men may be targeted.[17] It is for this reason that this thesis examines online sexual extortion as a wrong against individuals of any gender.

2.1.2 Literature on the Issues

2.1.2(a) Empirical Studies

Although legal literature on online sexual extortion is lacking, empirical research has been carried out on this conduct. Emphasis here is often placed on victim studies, prevention techniques, and educational awareness, with little mention of substantive criminal law.[18] Notable examples include surveys of child victims' experiences[19] of online sexual extortion and the Australian Institute of Family Studies Research Report into the harms of emerging

[14] ibid 122-124.
[15] B Wittes, "Cyber sextortion and international justice" (2017) 48 Georgetown Journal of International Law 941 at 944.
[16] Police Scotland news bulletin, "Men more likely to fall victim to sextortion" (14 Dec 2016). Available at: *http://www.scotland.police.uk/whats-happening/news/2016/december/men-more-likely-to-fall-victim-to-sextortion*; See also A Crawford, "British men 'increasingly' targeted by sextortion", BBC News, (25 May 2018). Available at: *https://www.bbc.co.uk/news/av/uk-44260271/british-men-increasingly-targeted-by-sextortion?intlink_from_url=https%3A%2F%2Fwww.bbc.co.uk%2Fnews%2Ftopics%2Fcgdz91y340mt%2Fsextortion&link_location=live-reporting-map*
[17] J Brown, "Experts warn of rise in internet blackmail as police probe suicide of Daniel Perry", The Independent, (16 Aug 2013). Available at: *http://www.independent.co.uk/news/uk/crime/experts-warn-of-rise-in-internet-blackmail-as-police-probe-suicide-of-daniel-perry-8769748.html*; *HM Advocate v Andrew McBride,* sentencing statement published on Judiciary of Scotland website per Lord Turnbull. Available at: *http://www.scotland-judiciary.org.uk/8/1360/HMA-v-ANDREW-MCBRIDE*
[18] See for example J Wolak and D Finkelhor, "Sextortion: findings from a survey of 1,631 victims" (Crimes Against Children Research Center, 2016). Available at: *https://www.wearethorn.org/wp-content/uploads/2016/08/Sextortion_Report.pdf*
[19] ibid.

technology in wider cases of sexual violence.[20] Such research tends to have specific aims, while no empirical research has been conducted in the UK on this problem. This leaves a gap in terms of knowledge of online sexual extortion practices and the impact on victims, which it is suggested could be filled through a combination of quantitative and qualitative research respectively.

2.1.2(b) Publicly Commissioned Reports

Similar issues arise in the context of publicly commissioned reports. The most significant research into the problem was published in the Europol report of 2017.[21] This addressed a number of issues, yet expressly excluded discussion of legislative responses.[22] Furthermore, the report is limited for the purposes of this research by focusing solely on offending against children. Despite this, the report found that the conduct "is heavily understudied"[23] and that "gaps in the research limit the capacity to develop evidence-based policies and interventions".[24] This supports the need for more studies on the issue, while reinforcing one of the problems that this research has found: that even among the small amount of literature that exists, most works only consider the impact on children.[25]

Even from a UK perspective, research has been limited. Although the Home Office undertook a broad review of cybercrime through a series of reports published in 2013, they omitted to consider online sexual offences at all, except those committed against children.[26] Likewise, a report produced by the Home Affairs Select Committee acknowledged the growing threat of online harms to individuals, but only made reference to certain types of

[20] N Bluett-Boyd, B Fileborn, A Quadara and S Moore, "The role of emerging communication technologies in experiences of sexual violence: a new legal frontier?" (Australian Institute of Family Studies Research Report No.23, 2013). Available at: *https://aifs.gov.au/publications/role-emerging-communication-technologies-experiences-sexual-violenc*

[21] Europol European Cybercrime Centre, *Online sexual coercion and extortion as a form of crime affecting children - Law Enforcement Perspective* (May 2017) at 6. Available at: *https://www.europol.europa.eu/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf*

[22] ibid at 8.

[23] ibid at 6.

[24] ibid.

[25] ibid; Wolak & Finkelhor (n.18); Home Office, *Cybercrime: a review of the evidence (Research Report 75), Ch 3, Cyber-enabled crimes – sexual offending against children* (Oct 2013); Bluett-Boyd et al B Fileborn, (n.20); Wittes et al (n.7); K Veli "Sexual extortion of children in cyberspace" (2016) 10 International Journal of Cyber Criminology 110.

[26] ibid Home Office.

conduct, omitting mention of sexual extortion.[27] The Law Commission has recently been asked to carry out a review into trolling, harassment and cyberbullying laws in England and Wales with a view to developing the UK government's Digital Charter but it is unclear that online sexual extortion will be included within the scope of this project.[28]

In Scotland, government-commissioned research has focused on similar areas and once again express reference to online sexual extortion is absent.[29] This is even the case in a recently published report on cybercrime, which although mentions extortion in an online context, states that "[t]here is very little known evidence in relation to extortion as a whole".[30] In light of these findings, there is a pressing need for a more comprehensive review of the problem in order to determine the scale of it and to identify possible responses.

2.2 Statistical Data

One problem mentioned above is that identifying instances of online sexual extortion is extremely difficult. There is little statistical data. This is characteristic of cybercrime more generally with it being difficult to accurately determine its prevalence.[31] It is suggested in this section that three factors explain why statistics are hard to come by. These are that there is no discrete offence of online sexual extortion, under-reporting, and problems with recording practices.

2.2.1 Lack of a Discrete Offence

The primary reason why it is so difficult to specifically map occurrences of online sexual extortion in Scotland is that there is no discrete offence of this name (or even sexual extortion). This problem is not limited to Scotland; in a US context it has been said that

[27] *Home Affairs Select Committee: E-crime* (2013, 5th Report of the Home Affairs Select Committee) HC 70 at 27. Reference was made to identity theft, phishing, clickjacking, romance frauds, cyberbullying and trolling.
[28] Law Commission press release, "Government asks Law Commission to look at trolling laws" (6 Feb 2018) Available at: *https://www.lawcom.gov.uk/government-asks-law-commission-to-look-at-trolling-laws/*
[29] Scottish Government, Crime and Justice, *Cyber-Crime in Scotland: A Review of the Evidence* (Mar 2018). Available at: *http://www.gov.scot/Resource/0053/00532978.pdf*
[30] ibid at 23.
[31] Gillespie, *Cybercrime* (n.2) 14.

"sextortion is not in the uniform crime statistics data. So, as a crime, it sort of doesn't exist".[32] However, although not a specific offence, the conduct is evidently criminal and can be prosecuted under a number of offences.[33] This makes it difficult to track individual instances in Scotland. This was acknowledged in the Europol report, which found there to be "shortcomings in the recording of incidents…which creates difficulties in assessing the scope of this crime threat."[34] Despite this, an attempt has been made in this chapter to glean from recent crime statistics the prevalence of this conduct, albeit that this analysis can only paint a very broad and sketchy picture.

2.2.2 Under-Reporting

Secondly, the very nature of the wrongdoing makes it liable to under-reporting.[35] Even where there are statistics aimed at measuring instances of this conduct, these may not be reliable.[36] Such cases often concern victims being made to provide images or perform sexual acts that are embarrassing, humiliating or degrading.[37] The fear of others discovering what has happened may deter victims from reporting. This was reflected in Police Scotland advice issued to child victims[38] and is an issue characteristic of extortion,[39] sexual offences,[40] and cybercrimes more generally.[41] Indeed academics have long recognised that extortion and blackmail are offences that are almost impossible for researchers to identify first-hand accounts of.[42] It is therefore unsurprising that where the conduct relates to all three areas, concerns arise as to the accuracy of any recorded figures.

---

[32] Wittes (n.15) at 943
[33] See Ch 3 for an overview of these offences.
[34] Europol, *Online sexual coercion* (n.21) at 7.
[35] D Wall "Cybercrimes and the Internet", in Wall, *Crime and the Internet* 8; Scottish Government, Crime and Justice, *Recorded Crime in Scotland: Other Sexual Crimes, 2013-14 and 2016-17* (Sep 2017) at 6. Available at: *http://www.gov.scot/Resource/0052/00525033.pdf*
[36] Gillespie, *Cybercrime* (n.2) 14.
[37] For a detailed discussion of these harms see below at 2.4-2.5.
[38] Police Scotland, "Police Scotland advice to child victims of online extortion" (20 Sep 2013). Available at: *http://www.scotland.police.uk/whats-happening/news/2013/september/advice-to-child-victims-of-online-extortion/*
[39] Scottish Government, *Cyber-crime* (n.29) at 23.
[40] T Thomas, *Reporting and Recording Sexual Offences* (2016) 8; S Pegg and A Davies, *Sexual Offences: Law and Context* (2016) 21.
[41] A Day, C Milmo, D Mort et al, "Scotland witnessing "significant" growth in cyber-crime", The Scotsman, (22 Jul 2017). Available at: *https://www.scotsman.com/future-scotland/tech/scotland-witnessing-significant-growth-in-cyber-crime-1-4511044*
[42] M Hepworth, *Blackmail* (1975) 5.

There are also a high number of child victims,[43] who may be less likely to report wrongdoing. A study into young victims' experiences of online sexual extortion among a group of 18-25 year olds found that only 16% of victims reported incidents to the police.[44] This may be for a number of reasons. Firstly, there may be a greater feeling of shame or embarrassment among children and the thought of their parents or the authorities knowing what they have gone through could be deeply traumatic.[45] Secondly, younger children may fail to appreciate the wrong they have suffered or even be aware that an offence has been committed.[46] Thirdly, further threats may be communicated following the criminal conduct, deterring reporting,[47] or they may be made to believe that they themselves have committed a criminal act.[48]

2.2.3 Recording Practices

One further issue is that regardless of how many offences are reported, how they are recorded is problematic. There is currently no distinction between offences committed online and offline in official statistics.[49] Although specific research was commissioned by the Scottish Government in respect of certain sexual offences committed online, this is not the norm when recording crime in Scotland. For the majority of offences it is not possible to determine from official statistics if an offence was committed online.[50] This is relevant as offences such as extortion and sexual offences can be committed both online and offline. Thus, the only measure of cybercrime in official statistics comes from offences that can *only* be committed online. These are primarily offences under the Computer Misuse Act 1990. However, this is a limited number of offences[51] comprising unauthorised access to computer material,[52] unauthorised access with intent to commit further offences,[53] and unauthorised

[43] Scottish Government, *Other Sexual Crimes* (n.35) at 6.
[44] Wolak & Finkelhor (n.18) at 6.
[45] ibid; Europol, *Online sexual coercion* (n.21) at 14.
[46] ibid Europol.
[47] Bluett-Boyd et al (n.20) at 37.
[48] See 1.3.3(b)(i)
[49] This was confirmed by Police Scotland in response to a Freedom of Information Request. See Day et al (n.41).
[50] ibid.
[51] Only 30 incidents under this statute were recorded for the period 2016-17: Scottish Government, *Cyber-crime* (n.29) at 8.
[52] Computer Misuse Act 1990 s.1(1).
[53] ibid s.2(1).

acts with intent to impair the operation of a computer.[54] As such, this statute is only really relied upon where there are no alternative offences to prosecute under, being described as a "stopgap".[55] One is therefore left guessing as to the prevalence of cybercrime in Scotland. This is despite the introduction of a "cyber-marker" for offences in April 2016:[56] this recording system has encountered difficulties and is still being developed and implemented.[57] The result is a lack of available evidence to help compare cyber and non-cyber instances of the same offence.[58] This is in contrast to England and Wales, where since 2015 there has been a specific requirement to record online offences separately, as reflected in their most recent national crime statistics.[59] As a result, Police Scotland lags behind forces in England and Wales when dealing with cybercrime, who are better placed to allocate resources to growing threats as determined through recorded data. These considerations therefore highlight the difficulties in relying on crime statistics when mapping the issue of online sexual extortion in Scotland.

2.2.4 Evaluation

However, this is not to say there are no useful statistics. Research was recently commissioned by the Scottish government in relation to sexual offences and the impact of the Internet. There was found to be a sharp increase in the number of cyber-enabled sexual offences, with the findings being published in a report entitled *Recorded Crime in Scotland: Other Sexual Crimes, 2013-14 and 2016-17*.[60]

The report dealt with "other sexual crimes", a category made up of 41 different offences. Despite this, the offences of communicating indecently, causing a person to view sexual activity or images, possession of indecent photos of children, sexual activity with older children, sexual exposure, public indecency, and voyeurism made up 94% of the offences recorded in the 2016-17 time period.[61] These are (as shown in the next chapter) the very offences likely to capture conduct typically seen in online sexual extortion cases. From 2015-

[54] ibid s.3(1), (2).
[55] Gillespie, *Cybercrime* (n.2) 14 citing *Home Affairs Select Committee: E-crime* (n.27).
[56] Scottish Government, *Cyber-crime* (n.29) at 65.
[57] ibid at 18.
[58] ibid at 11.
[59] ibid at 19.
[60] Scottish Government, *Other Sexual Crimes* (n.35).
[61] ibid at 10.

16 onwards, this category of "other sexual crimes" has become most prevalent in Scotland, overtaking sexual assault.[62] This comes against the backdrop that sexual offences are at their highest recorded level in this country since 1971 (the earliest point with which direct comparisons are possible).[63]

In addition to the growing number of sexual offences being recorded, use of emerging technologies and the Internet can be identified as factors in the increase of "other sexual crimes". Many of these offences (e.g. communicating indecently; causing a person to engage in sexual activity) can be committed online. The most recent figures show that over half of "other sexual crimes" are now cyber-enabled, increasing from 38% in 2013-14 to 51% in 2016-17.[64] These statistics point towards a change in the nature of sexual offending. Furthermore, in most cases the perpetrator and victims were strangers with no prior contact (online or offline) before the offence itself was committed.[65] This again can be explained by the use of technology, where physical conduct is not required before a sexual offence is committed.

What is also interesting are trends relating to extortion and threats. Between 2016-17 there was a 9% increase in offences recorded as "other violence" within the over-arching category of "non-sexual crimes of violence."[66] The research found this to be the result of significant rise in recorded cases of threats and extortion, which rose by 25% from the previous year.[67] This again reflects the growing trend of such offences to be committed online, as the Internet has developed into a vehicle through which threats and extortion can easily be communicated.[68]

On evaluation of these statistics, online criminal sexual activity can be seen as a growing problem in Scotland. Although increased recording of certain crimes could be down to greater willingness among victims to report, increased offending remains a likely

[62] ibid at 6.
[63] Scottish Government, Crime and Justice, *Recorded Crime in Scotland, 2017-18* (Sep 2018) at 2. Available at: *https://www.gov.scot/binaries/content/documents/govscot/publications/statistics/2018/09/recorded-crime-scotland-2017-18/documents/recorded-crime-scotland-2017-18/recorded-crime-scotland-2017-18/govscot%3Adocument/recorded-crime-scotland-2017-18.pdf?forceDownload=true*
[64] Scottish Government, *Other Sexual Crimes* (n.35) at 4.
[65] ibid at 17.
[66] Scottish Government, Crime and Justice, *Recorded Crime in Scotland, 2016-17* (Sep 2017) Available at: *http://www.gov.scot/Resource/0052/00525033.pdf* at 21.
[67] ibid. These are the most recent statistics to include specific figures on extortion and threats.
[68] See below at 2.4.2.

explanation.[69] That online sexual extortion is a very real threat can be seen from the figures analysed above and the following findings. Firstly, sexual offences are at their highest rate in Scotland and the most prevalent sub-category is "other sexual crimes". These offences are those that would typically be charged in online sexual extortion cases. Secondly, the growth of cyber-enabled crime can be attributed towards this change, and this increase is the result of a higher proportion of online offences being reported. This represents a changing pattern in the way sexual offenders are operating in Scotland with online offending now being far more prevalent. Thirdly, there has been a rise in threats and extortion, which are defining elements in these cases.

Thus, despite there being no official recorded figures for online sexual extortion, trends can be identified from related offences that perpetrators may be charged with. These patterns point towards an increasing likelihood that instances of this conduct in Scotland are steadily growing.

2.3 Media Reporting

In mapping online sexual extortion in Scotland, the previous sections have exposed two problems. Firstly, limited reference is made to the conduct in existing literature, and secondly, for the reasons outlined above, there is a lack of recorded statistics dealing specifically with the conduct. Both issues make it difficult to evaluate the scale of the threat in Scotland and for law enforcement bodies to suitably address it.[70] However, it will be shown that media coverage can be of some assistance.

The issue was brought to public attention in Scotland through the high-profile reporting of the death of 17 year old, Daniel Perry, who took his own life in 2013 after falling victim to an online sexual extortion scam. Perry was tricked into creating and uploading explicit videos of himself online,[71] and was then threatened through Skype that the material would

[69] L Campbell and S Cowan, "The relevance of sexual history and vulnerability in the prosecution of sexual offences", in P Duff and P Ferguson (eds), *Scottish Criminal Evidence Law: Current Developments and Future Trends* (2018) 67 at 69.
[70] D Wall, *Cybercrime: The Transformation of Crime in the Information Age* (2007) 20.
[71] D Lee, "Teenager's death sparks cyber-blackmailing probe", BBC News (16 Aug 2013). Available at: *http://www.bbc.co.uk/news/uk-scotland-edinburgh-east-fife-23712000*

be disseminated unless a sum of money was paid to the perpetrator.[72] Although a high-profile story, this is not an isolated example. Another Scottish case reported in the press is that of Andrew McBride who carried out online abuse over a five year period with 42 known victims.[73] Other local reports have suggested that such conduct has been carried out across the jurisdiction, even on a smaller scale. These include advice from Police Scotland following offending in Lanarkshire,[74] and an article warning of ongoing activity in Angus.[75] Although this activity may not be reflected in literature or official crime statistics,[76] media coverage and reporting of these cases nevertheless help raise awareness of the issue. These allow us to identify patterns and trends in conduct and, as such, are of great benefit in identifying possible responses.

These examples have, in part, contributed towards the issue recently being publicised in the UK media and among law enforcement bodies. The NCA released a video warning individuals of the dangers of online sexual extortion.[77] Similarly, the BBC reported on the issue and interviewed victims just this year.[78] This has had the positive impact of increasing awareness, particularly among children. However, it is difficult to evaluate the practical effect of such campaigns, particularly in light of the above findings relating to the lack of statistics and recording of this conduct.

2.4 Exploring the Harms

This section will examine the harms of online sexual extortion. The purpose here is to identify the types of harm caused. This will lay the foundations for the third chapter where the criminal law response will be evaluated.

---

[72] A Cramb, "Teenage committed suicide 'after being blackmailed on Skype'", Daily Telegraph (15 Aug 2013). Available at: *https://www.telegraph.co.uk/news/uknews/crime/10245809/Teenager-commited-suicide-after-being-blackmailed-on-Skype.html*

[73] "Andrew McBride jailed for online sexual blackmail campaign", BBC News (14 Jan 2015). Available at: *http://www.bbc.co.uk/news/uk-scotland-glasgow-west-30814443*

[74] Police Scotland news bulletin, "Webcam extortion warning – Lanarkshire" (23 August 2016). Available at: *http://www.scotland.police.uk/whats-happening/news/2016/august/webcam-extortion-warning-lanarkshire*

[75] G Brown, "Sextortion scammers targeting Angus residents in 'nasty' con", The Courier (20 July 2018) Available at: *https://www.thecourier.co.uk/fp/news/local/angus-mearns/691358/sextortion-scammers-targetting-angus-residents/*

[76] See 2.2-2.2.3

[77] NCA information page on "Sextortion". Available at: *https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/kidnap-and-extortion/sextortion-webcam-blackmail*

[78] D Whitworth, "Sextortion: big rise in victims 'with tens of thousands at risk'", BBC News (24 May 2018). Available at: *https://www.bbc.co.uk/news/newsbeat-43433015*

The types of harms are varied and manifest themselves in a number of ways. This section will begin by charting the development of sexual extortion and show how the Internet and technological advancements have changed the nature of this offending. It will be argued that as a result of this, online sexual extortion represents a new and very specific type of wrong that can be differentiated from sexual extortion.

Following this, the focus will turn to the specific harms in assessing which interests online sexual extortion violates. The following harms will be addressed: sexual harm, damage to privacy and reputation, and financial harm.

2.4.1 Development of Sexual Extortion

This thesis considers the threat of online sexual extortion as a particular species of harm in Scotland. However, why is the focus limited to online conduct? Sexual extortion occurs in a number of contexts in the offline world[79] and has "taken place as long as people have had the power to demand sex from one another on threat of doing each other harm".[80] Recorded accounts of sexual blackmail can be traced back as far as the 18th century, becoming increasingly prominent in the Victorian era.[81] As a result, sexual blackmail has been recognised as a subset of blackmail itself.[82] Sexual extortion is not limited to instances where a sexual act is demanded or where the threat is to sexually assault the victim, but also where – regardless of whether the demand is sexual - the threat is to expose something sexual. This is consistent with the broad definition of online sexual extortion adopted in Chapter 1.

This conduct has historically been seen in the context of sexuality with male victims being targeted through threats to expose their sexuality.[83] This has been attributed to its recognition as a more serious crime during the 20th century.[84] Greater attention has been paid in recent years in the area of IBSA.[85] Sexual extortion in this context may occur where former partners

[79] See International Association of Women Judges (IAWJ), *Stopping the Abuse of Power Through Sexual Exploitation: Naming, Shaming and Ending Sextortion* (2012) for examples of this.
[80] Wittes et al (n.7) at 11.
[81] A McLaren, *Sexual Blackmail: A Modern History* (2002) 3.
[82] Hepworth, *Blackmail* (n.42) 8, where the author lists "sexual blackmail" as a specific type of blackmail. For a detailed treatment of the historical development of sexual blackmail see McLaren ibid.
[83] See McLaren's statement that "The homosexual man was the classic prey of extortionists" ibid 6. See also *R v Stone* (1989) 11 Cr.App.R.(S.) 176 for an example of this.
[84] P Alldridge, "Attempted murder of the soul: blackmail, privacy and secrets" (1983) 13 OJLS 368 at 383.
[85] See the recent introduction of statutory offences for this conduct: Criminal Courts and Justice Act 2015 s.33 in England and Wales; Abusive Behaviour and Sexual Harm (Scotland) Act 2016 s.2.

threaten to expose sexual images of the victim. However, even beyond these specific circumstances, case reports demonstrate that sexual extortion is by no means a new species of offending. An example is the English case of *R v Hadjou*[86] from 1989, where the defendant filmed consensual sex with the victim and threatened to send copies of this film to her employer unless she paid him £2,500. Similarly, sexual photographs were used to extort sums of money from victims in both the Scottish case of *White v HM Advocate*,[87] and English case of *R v Kewell*.[88] This shows that even before the growth of the Internet and other technological advancements sexual extortion occurred and is by no means novel. However, what has changed is how this conduct is perpetrated. In light of this, the ways in which technological developments have altered this type of offending, along with the impact of these developments, will now be considered.

2.4.2 Significance of the Cyber Element

The development of the Internet and technological devices has enabled sexual offences to be perpetrated in a number of ways.[89] Technology not only acts as a vehicle through which abuse may be carried out, but in itself represents an additional threat to a victim's personal autonomy and liberty.[90] This is particularly so in the context of sexual extortion and in this section it will be argued that there are sufficient differences in the nature of offending and the types of harm to support the need for a discrete examination of online sexual extortion.

'Cybercrime' was initially conceived of as a discrete category of offences that could be committed using a network computer.[91] However, as technology progressed and devices became more sophisticated, computers - and the Internet - began to be used in different ways. As a result, they became a medium by which traditional criminal offences could be committed and "given a new lease of life".[92] This led to a divergence in cybercrime treatment

[86] (1989) 11 Cr. App. R. (S.) 29.
[87] [1999] 4 WLUK 327.
[88] [2000] 2 Cr. App. R. (S.) 38.
[89] C McGlynn and E Rackley, "Image-based sexual abuse" (2017) 37 OJLS 534 at 534.
[90] Powell & Henry (n.5) at 410.
[91] D Wall, "Criminalising cyberspace: the rise of the Internet as a crime problem", in Y Jewkes and M Yar (eds), *Handbook of Internet Crime* (2013) at 95; Wasik, *Crime and the Computer* (n.2)
[92] Y Jewkes and M Yar, "Introduction: the Internet, cybercrime and challenges of the twenty-first century", in Jewkes & Yar, *Handbook of Internet Crime* ibid at 3.

between those offences that could be committed *only* through the use of technological devices, and those that could be committed both with and without their use. Cybercrime is now viewed as an overarching category including a broad spectrum of criminal conduct.[93] Discussion tends to be structured according to how wrongs are perpetrated. The primary distinction widely adopted among academics is between cyber-enabled and cyber-dependent crimes.[94] However, terminology here is overlapping and other works have categorised the conduct using the terms "tool cybercrimes", "target cybercrimes" and "computer-incidental cybercrimes".[95]

This leads us to the broader question of why online sexual extortion should be considered as a distinct wrong. It has been stated that "'computer crime' is not…a precise legal category"[96] and that no distinction should be drawn between criminal conduct committed through the use of a computer, and equivalent conduct occurring without.[97] This is because the only difference is the medium; other than this "the crime is fundamentally familiar".[98] However, this is an outdated position. Recognising that an offence is committed online is important.[99] This is because "it captures the different ways the Internet exacerbates the injuries suffered".[100] Furthermore, legislatures and policymakers have faced criticism for treating emerging technology as 'tools' of abuse, as such an approach can "elide the unique ways in which victim survivors experience harms",[101] while having a distinct online label better allows law enforcement agencies to monitor the prevalence of online conduct and to allocate resources towards tackling cybercrime.[102]

Specifically, a number of features of online sexual extortion distinguish it from 'real world' sexual extortion. This section will draw on some of Clough's key features of cybercrime[103] and examine how they specifically apply in the context of online sexual extortion. These

[93] Gillespie, *Cybercrime* (n.2) 3.
[94] Clough, *Cybercrime* (n.2) 11. Clough lists the UK, the US, Canada and Australia as adopting this classification or a variant thereof.
[95] Bremner, *Cybercrime* (n.3) 39.
[96] Wasik, *Crime and the Computer* (n.2) 1.
[97] ibid.
[98] P Grabosky, "Virtual criminality: old wine in new bottles" (2001) 10 Social and Legal Studies 243 at 243
[99] Citron, *Hate Crimes* (n.2) 4.
[100] ibid.
[101] Powell & Henry (n.5) at 398.
[102] See above at 2.2.3.
[103] Clough, *Cybercrime* (n.2) 5.

include: (a) the ease with which the conduct can materialise and develop; (b) the potential for anonymity; (c) the scale of the conduct; and (d) the permanence of the harm.

2.4.2(a) Ease

One striking difference between online sexual extortion and equivalent offline conduct is the ease with which online conduct can take place. It can happen very quickly and requires little effort on the part of the perpetrator. This can be attributed to factors such as increased literacy and advances in communications technology facilitating extortion.[104] A false identity (which may previously have taken some effort or even criminal connections to come by) can be acquired online in a matter of minutes by creating a false email account.[105] When coupled with the speed at which images can be uploaded, or messages sent, this provides ample opportunity for sexual predators to operate and target vulnerable individuals. It has made possible the emergence of the "full-time criminal blackmailer",[106] which would previously have been unlikely.

Taking this further, it is more than simply the emergence of IT and the worldwide web that has allowed sexual extortion to flourish. Social media provides a much easier avenue through which to target victims, including WhatsApp, Facebook, Snapchat or any number of applications that are routinely used. There are continually new media platforms emerging that offer additional opportunities to engage in this conduct (e.g. web-based chat rooms; online dating websites) and these multiply avenues through which perpetrators can engage in online sexual extortion and target more victims. The implications in terms of privacy are striking with these being described as a "veritable treasure trove of personal information",[107] providing unprecedented means of accessing personal data. Such information is a powerful weapon for perpetrators who may be able to use this not only against the victim in extorting them, but also to build rapport with them. There is also the possibility of more easily communicating (or threatening to communicate) with relatives, parents, friends and colleagues. Once again this can be attributed to the growth of social media and the ease of accessing personal data online. The thought of a victim knowing that these individuals may

[104] Hepworth, *Blackmail* (n.42) 22.
[105] Clough, *Cybercrime* (n.2) 7.
[106] M Hepworth, cited in news report, The Times, 19 Aug 1986, cited in Wasik, *Crime and the Computer* (n.2) 153.
[107] Clough, *Cybercrime* (n.2) 418.

become involved in the conduct only adds to their suffering, demonstrating the additional harm to victims that technology may facilitate.

2.4.2(b) Anonymity

The degree of anonymity that technology offers is another factor that increases the likelihood of this conduct being carried out in the ways illustrated in this thesis. Extortion and blackmail have always been considered highly secretive offences,[108] explaining why they are greatly underreported.[109] This effect is exaggerated in cyberspace as it "affords offenders unprecedented opportunities to disguise and distort their identities".[110] The impact is that the criminal law cannot perform its core functions of communicating norms, deterring criminals, or remedying harms if those perpetrators cannot be identified.[111]

The relevance of anonymity is twofold. The first relates to the perpetrator. The ability to remain anonymous is "empowering";[112] offenders may feel less bound by moral or social constraints.[113] Anonymity can increase confidence when it comes to sending messages or threatening the victim. Perpetrators may also pursue and engage in fantasies that they otherwise would not in person. It is for these reasons that technology has been said to be "a unique medium for social shaming".[114]

On the other hand, from the victim's perspective, individuals appear more likely to participate in risky behaviours online than they would offline.[115] This has been termed the "online disinhibition effect".[116] Face-to-face, a person would be reluctant to allow a stranger to see intimate images of them or to engage in sexual activity for the benefit of a stranger; in the online environment there is less concern. This has been partially attributed to a greater disregard for social norms,[117] creating a degree of freedom to do whatever one wants to do.[118]

---

[108] Hepworth, *Blackmail* (n.42) 22.
[109] ibid 35.
[110] Jewkes & Yar (n.91) at 3.
[111] Citron, *Hate Crimes* (n.2) 142.
[112] M Cross, *Social Media Security* (2014) 170.
[113] Clough, *Cybercrime* (n.2) 418.
[114] A Powell and N Henry, "Embodied harms: gender, shame, and technology-facilitated sexual violence" (2015) 21 Violence Against Women 758 at 767.
[115] A Barak, "Sexual harassment on the Internet" (2005) 23 Social Science Computer Review 77 at 82.
[116] J Suler, "Online disinhibition effect" (2004) 7 Cyber Psychology & Behavior 321.
[117] ibid.
[118] A Ben-Ze'ev, "Privacy, emotional closeness, and openness in cyberspace" (2003) 19 Computers in Human Behavior 457 at 464.

This is supported by psychiatric research, which has found that the combination of anonymity and lack of face-to-face contact "can easily lead to a loss of normal social inhibitions and constraints".[119] This results in a greater likelihood of emotional self-disclosure, especially where such disclosure is contrary to accepted moral norms.[120] It is not necessarily the disclosure of sexual material that may provide the foundation for extortion. The victim may reveal intimate details about themselves relating to their wider sexuality and later be coerced through the threatened disclosure of these details.

These two aspects of anonymity have been referred to as "benign disinhibition" and "toxic disinhibition".[121] Both present real problems and together have the effect of creating more confident perpetrators who are willing to go further than they likely would in an offline setting, and victims who are more likely to share information and sexual material to the benefit of these perpetrators.

2.4.2(c) Scale and Reach

Perhaps the most striking feature of digital conduct is its potential scale. Although large-scale extortion operations may theoretically occur in an offline context, it would be extremely difficult to match the scale of online operations. An example can be seen in ***R v. Miller***[122] where the accused targeted over 300 victims, many of whom were coerced into sending sexually explicit images or videos which he threatened to distribute if they did not comply with further sexual demands.[123]

Perpetrators also operate across different jurisdictions. The Internet provides the means to invade someone's life from another jurisdiction and "enables diffuse, viral communication from one platform to another, and from one individual to another".[124] This would simply not be achievable without using technology. Why this is significant? Firstly, technology enables perpetrators to cast their net wide, and secondly, it has the potential to frustrate the enforcement of laws. With respect to enforcement, three issues arise: identification of the

[119] M G McGrath and E Case, "Forensic psychiatry and the Internet" (2002) 30 J Am Acad Psychiatry Law 81 at 85.
[120] Ben-Ze'ev (n.118) at 457.
[121] Suler (n.116) at 321.
[122] 2011 ABPC 354.
[123] ibid.
[124] Bluett-Boyd et al (n.20) at 3.

perpetrator, cross-jurisdiction collaboration, and enforcement of the laws.[125] It is entirely conceivable that perpetrators will target individuals in those jurisdictions where there is less chance of them being brought to justice. The ability to target a large number of victims has therefore allowed online sexual extortion to become a growing threat. This is partly related to the ease with which perpetrators can act. Perpetrators now attempt to contact and draw in more victims than before and there really is no limit to the number of individuals that may be targeted.[126]

However, it is not simply the ability to target victims that is concerning. Outlets exist whereby sexual predators can work as part of a network or encourage one another. These have been described as "support groups for previously isolated sexual predators, support that has the potential to encourage some individuals to act on fantasies that would otherwise remain dormant".[127] A driving motivation behind this conduct is for individual members of such communities to enhance their status and reputation.[128] Such conduct may go beyond the publication of material obtained through extortion and victims may be extorted live on webcam.[129] Existing research has found that "when such materials are considered new or rare, they facilitate admission of new members or raise the reputation of the existing ones in online groups formed by abusers".[130] An example is in the aforementioned case of Matthew Falder. In addition to carrying out online sexual extortion, he circulated material among 'hurtcore' websites where sexual predators, abusers and paedophiles share images of sexual abuse or physical harm. This is done in a competitive manner: "total control over victim makes the abuser feel psychologically superior and this feeling of superiority might satisfy him/her so much that physical sexual abuse becomes needless or undesirable".[131] The resultant harm can be severe. There is no real way for the victim to determine who has seen their images, where they have been uploaded, and how they have been used. This adds a new dimension to the criminality and "the anonymity of the Internet has allowed those with rare

[125] Substantive laws and also those relating to jurisdiction and extradition.
[126] W L Robinson, "Digitizing privacy", in A E Cudd and M C Navin (eds), *Core Concepts and Contemporary Issues in Privacy* (2018) 189 at 192.
[127] McGrath & Case (n.119) at 85.
[128] Europol, *Internet Organised Crime Threat Assessment (IOCTA) Report* (2017) at 38. Available at: https://www.europol.europa.eu/sites/default/files/documents/iocta2017.pdf
[129] Powell & Henry, *Sexual Violence* (n.13) 127.
[130] Veli (n.25) at 112.
[131] ibid at 120.

or bizarre sexual needs a place to find 'virtual' companionship, validation, and possibly an outlet for their paraphilias".[132]

2.4.2(d) Permanence

In terms of permanence, online conduct may involve a more persistent degree of control. This has similarly been found to be true of cyberstalking, where technology has provided continual access to victims.[133] The impact in this context has been increased feelings of fear, exposure and vulnerability.[134] Additionally, how the conduct is perpetrated online can be viewed as an aggravating factor in contrast to other cases of sexual extortion. This is considered in an article examining the ways in which technology facilitates sexual violence with it being stated that "once something is "out there" on the web it is very difficult to remove, with it being said to be impossible to fully remove content from the Internet".[135] In one case where sexual photographs of the victim were uploaded to a pornographic website they were viewed over 1,000 times before being removed.[136]

The permanence can also be seen by reference to the communication between perpetrator and victim: "modern communications provide both immediacy and distance".[137] Although demands or threats occurring offline may be regular, it is difficult to envisage how they could reach the degree of regularity as through the use of technology. Victims can be targeted while at home, at work, and potentially at every point during their day. As a result the conduct has been labelled as a form of "sexual slavery".[138] There is little chance of escaping the threats and the continuous and unrelenting nature of the harm is illustrated in *R v Casabolt*[139] where the defendant tried to extort £2 million from his estranged wife. In doing this, he threatened her by stating: "If my terms are not met, I can keep triggering the public with information about you for years, whipping them up into a frenzy."[140] This demonstrates the potential for long-lasting harm, and for the harms to multiply with every future non-consensual viewing or dissemination of sexual material belonging to the victim. This shows

[132] McGrath & Case (n.119) at 85.
[133] Powell & Henry (n.5) at 409.
[134] ibid.
[135] Bluett-Boyd et al (n.20) at 36.
[136] *R v Casabolt* [2016] EWCA Crim 1377 at para 9.
[137] Clough, *Cybercrime* (n.2) 417.
[138] Wittes (n.15) at 945.
[139] Supra n.136.
[140] ibid at para 8.

that technology has not only made it possible for victims to be targeted in a more pervasive manner, but that there are now severe "ongoing ramifications for our behaviour in a way that would not have previously been possible".[141] This can be seen as one of the greatest differences in the nature of harm suffered by victims of online sexual extortion.

2.5 Identifying the Harms

Having established the ways in which the Internet and technological advances have allowed online sexual extortion to develop and why it is distinguishable from extortion in an offline context, this section will now consider the nature of the harms themselves. This will be done in order to show the following:

(i) that online sexual extortion cannot simply be categorised as one type of offence,
(ii) that the harms experienced in one case of online sexual extortion may differ from those experienced in another, and
(iii) that this consequently makes it difficult when identifying the most appropriate legal responses to the conduct.

The following harms have been identified and will be addressed in turn: (i) sexual harm, (ii) damage to privacy and reputation, and (iii) financial harm.

2.5.1 Sexual Harm

A constituent component of online sexual extortion is the 'sexual' element. Violation of sexual autonomy distinguishes this conduct from other types of extortion. This section will consider the nature of these harms and assess (i) whether or not online sexual extortion can correctly be labelled a 'sexual offence' and (ii) the impact of this conclusion. This will be done by reference to literature on sexual offences and key underlying principles including

[141] Bluett-Boyd et al (n.20) at 23.

sexual autonomy and consent. Green proposes three separate categories of sexual offences and reference to these will be helpful in differentiating between the varying types of sexual harm.[142] These are offences involving the prohibition of one or more type of sexual conduct, conduct deemed preparatory of, or conducive to, future sexual wrongs, and conduct infringing an aspect of one's right to sexual autonomy.[143]

2.5.1(a) <u>What are the Harms?</u>

Online sexual extortion evidently has the potential to violate one's sexual autonomy. What is meant by sexual autonomy? In their recent reform of sexual offences in Scotland, the SLC stated that "autonomy is a complex idea but in the context of legal regulation of sexual conduct it involves placing emphasis on a person freely choosing to engage in sexual activity".[144] This idea of free will is central to the concept and operates on two levels: that an individual should be free to engage in consensual sexual activity unless there is good reason prohibiting this, and it should be a recognised wrong where an individual is made to participate in sexual activity against their free will.[145] These two aspects have been referred to respectively as the positive and negative dimension of autonomy.[146] The most relevant dimension in this context is the negative one. The core sexual wrong in most cases is that an individual is made to engage in sexual activity against their free will as a result of a demand backed by a threat, or that their sexual autonomy is infringed through failure to comply with demands. However, that is not to say that no threat is posed to an individual's positive sexual autonomy. Conduct may have a wider impact to the extent that where an individual is coerced using sexual material sent to another in good faith, the threat of sexual extortion may deter individuals from expressing their sexual autonomy in a positive manner.

It is recognised that in some cases even before there is any coercion (or even contact between victim and perpetrator), a victim's sexual autonomy may be violated. An example

[142] S Green, "What are the sexual offences?", in C Flanders and Z Hoskins (eds), *The New Philosophy of Criminal Law* (2016) 57.
[143] ibid at 60.
[144] Report on *Rape and Other Sexual Offences* (Scot Law Com No 209, 2007) para 1.25.
[145] ibid.
[146] A Wertheimer, "Consent to sexual relations", in A Wertheimer and F Miller (eds), *The Ethics of Consent: Theory and Practice* (2009) 195 at 196.

of this would be where the perpetrator hacks the victim's webcam and uses this to watch and record sexual activity. Although a serious wrong, this falls under Green's second category of sexual offences as "conduct that is presumed to be preparatory of, or conducive to, future (illicit) sexual conduct".[147] This section is more concerned with the specific harms involved in online sexual extortion, rather than preliminary or incidental breaches of sexual autonomy that may occur in the process of committing extortion.

It has been shown in this thesis that perpetrators employ "non-physical forms of coercion online to extort sexual favours from the victim".[148] It must be stressed that the lack of physical contact between victim and perpetrator does not lessen the severity of the harm. There is concern that where victims yield to sexual activity as a result of coercive power, the lack of physical force may make them fear that the activity will be viewed as consensual.[149] This non-consensual sexual conduct still constitutes a serious wrong. What is required is a change in entrenched perspectives that sexual abuse or violence necessarily requires physical conduct.[150] This is because they "invade a deeply personal zone, gaining non-consensually that which should only be shared consensually".[151] Such activity should still be referred to as 'sexual violence' and work continues to be done to "widen narrow definitions, based on the idea that violence is a physical manifestation, to include emotional, sexual, financial, economic and psychological abuse".[152] One impact of this is that it may help to ensure that wider forms of coercion (e.g. extortion) are treated as invalidating consent.[153]

Additionally, in terms of harms, breach of sexual autonomy may cause not only physical harm, but also psychological (including humiliation and degradation),[154] which in turn explains the importance of treating sexual offences committed without physical contact as seriously as physical sexual wrongs. In *R v Egege* the victim was found to have experienced anxiety and distress following the hacking and extortion she experienced,[155] while one

[147] See above at 1.3.4; Green (n.142) at 60.
[148] Police Scotland, *Scottish crime recording standard and Scottish government counting rules* (Apr 2019) at 48. Available at: *https://www2.gov.scot/Resource/0054/00547065.pdf*
[149] IAWJ, *Stopping the Abuse of Power Through Sexual Exploitation* at 30.
[150] C McGlynn, E Rackley and R Houghton, "Beyond 'revenge porn': the continuum of image-based sexual abuse" (2017) 25 Feminist Legal Studies 25 at 35.
[151] J Horder, *Ashworth's Principles of Criminal Law,* 9th edn (2019) 344.
[152] M Todd, "Virtual violence: cyberspace, misogyny and online abuse", in T Owen, W Noble and F Speed (eds), *New Perspectives on Cybercrime* (2017) 141 at 145.
[153] L Farmer, *Making the Modern Criminal Law* (2016) 290.
[154] Horder, *Principles* (n.151) 345.
[155] *R v Egege* [2017] EWCA Crim 2161 at para 5.

survey of young online sexual extortion victims found that 24% of respondents had to seek mental health advice following abuse.[156]

Harms vary according to the nature of the wrongful conduct. Where a sexual demand is made, consent will likely be vitiated as a result of the threat. Demands broadly fall into two categories. The first is where the perpetrator demands through threats that the victim engages in sexual activity (either in person or through a technological device). The second is where the demand does not involve the victim engaging in live sexual activity for the perpetrator, but rather is to supply sexual material relating to the victim or third party.

Where faced with a sexual threat, victims may suffer a different type of sexual harm from that discussed above. It may, for example, be that the perpetrator has threatened physical sexual harm against the victim (or another) unless they comply with their demands. However, just as in the case of demands, threats may nevertheless be of a sexual nature without involving physical harm. It may be that the perpetrator threatens to expose sexual material of the victim or information related to their sexuality.

2.5.1(b) Online Sexual Extortion as a Sexual Offence

It will be argued that online sexual extortion should be categorised as a sexual offence. Law enforcement bodies must not lose sight of the 'sexual' wrongs present in such cases. Although this may seem an academic point, whether or not an offence can be said to be 'sexual' is significant in practice. There are two aspects to this. The first concerns criminal liability and has implications in terms of fair labelling. The second concerns procedural rules and notification requirements.

The starting point is that an individual may only be convicted under the Sexual Offences (Scotland) Act 2009 where they commit a sexual wrong. Certain offences in the 2009 Act (e.g. rape) are inherently sexual and require no further proof of this, yet others[157] require that

[156] Wolak & Finkelhor (n.18) at 5.
[157] E.g. sexual coercion and coercing a person into being present during sexual activity. See Gordon, *Criminal Law* (n.1) para 38.01.

an element of the wrongful conduct in question be 'sexual'.[158] While this may seem an obvious requirement, it is important to stress that this is determined objectively, the test being whether "a reasonable person would, in all the circumstances of the case, consider it to be sexual".[159] That this is determined objectively is to its benefit. This has the effect that where the accused carries out an act without obtaining sexual gratification (such as in purely financially motivated cases), but the victim suffers an infringement of their sexual autonomy, the act is correctly labelled as 'sexual'.[160]

There are important implications where an individual has specifically been convicted of a sexual offence. The most striking is being labelled a 'sexual offender'. This has the benefit of alerting others to both the nature, and degree, of culpability of the convicted individual. This can be seen as being of symbolic importance[161] in ensuring that the offender is identified as having committed a sexual wrong. As will be seen in the third chapter, this may be lost where the offender is convicted of an offence such as extortion which fails to reflect this.

However, recognition of criminal conduct as 'sexual' also has practical consequences. In terms of disposal, an offender may be made subject to the notification procedure.[162] This is regulated by the Sexual Offences Act 2003, with Schedule 3 listing those offences which can trigger this procedure.[163] Although under English law the Schedule provides an exhaustive list of offences, in Scotland there is a residual category that includes an offence other than that listed in the provision where the court determines "that there was a significant sexual aspect to the offender's behaviour in committing the offence".[164] This is a striking difference between the two jurisdictions. This means that in Scotland, even if an individual has not been convicted of a sexual offence, notwithstanding this, they may still be subject to the notification requirements. This is significant in terms of online sexual extortion. It allows for an individual who is convicted of extortion, where there is a "significant sexual aspect to the offender's behaviour in committing the offence",[165] to be treated as a sexual offender.

[158] 2009 Act s.60(2).
[159] ibid.
[160] Gordon, *Criminal Law* para 38.01.
[161] J Chalmers and F Leverick, "Fair labelling in criminal law" (2008) 71 MLR 217 at 226ff
[162] See Home Office, *Explanatory Notes to the Sexual Offences Act 2003* para 149: "this process is commonly known as "registration", and often referred to loosely as creating a "sex offenders register"".
[163] Sexual Offences Act 2003 Schedule 3.
[164] ibid para 60.
[165] ibid.

The result is that there is less concern where the perpetrator is not convicted of a sexual offence, but is convicted of another offence, as some of the same practical outcomes can be achieved.[166]

What does this mean in practice? The consequences of being subject to the notification requirements were strengthened considerably the 2003 Act[167] and there now exists an "armoury of special measures developed to register, track, and control actual and potential offenders".[168] These are contained in Part 2 of the 2003 Act and apply in Scotland.[169] Where an offender is over 18 and sentenced to a term of at least 30 months imprisonment then the notification requirements are imposed for an indefinite period.[170] Full details are beyond the scope of this research but can be found in the Part 2 of the Act and also on Police Scotland's webpage on Registered Sex Offender Management.[171]

Characterising this as a sexual offence also has procedural implications. These include that courts may pass an extended sentence (which is only possible in respect of sexual offences tried on indictment),[172] the complainer may be treated as a vulnerable witness[173] and receive special protections at trial,[174] and the defence may be prohibited from asking questions relating to the character of the complainer[175] (including previous sexual conduct).[176]

While these mechanisms may still be available in non-sexual offence cases, again by reference to the test of whether there was a "significant sexual aspect" to the offending, this is not automatic from the outset of proceedings, would have to be done by application or assessed, and would not therefore provide the same guaranteed level of protection as complainers in sexual offences cases receive.

---

[166] Report on *Rape and Other Sexual Offences* (n.144) para 3.43.
[167] P Rook and R Ward, *Rook & Ward on Sexual Offences: Law and Practice*, 5th ed (2016) para 35.03-35.04.
[168] Farmer, *Modern Criminal Law* (n.153) 291.
[169] 2003 Act s.142(3)(a).
[170] ibid s.82(1).
[171] Police Scotland webpage, "Registered Sex Offender Management". Available at: *https://www.scotland.police.uk/about-us/police-scotland/specialistcrime-division/national-offender-management-unit-new/registered-sex-offender-management*
[172] Criminal Procedure (Scotland) Act 1995 s.210A(xxviii)
[173] ibid s.271
[174] ibid s.271H
[175] ibid s.274(1)
[176] ibid s.274(1)(b)

It is for these reasons and those related to the labelling and culpability of the accused, that show the need for online sexual extortion to be treated as a sexual wrong and for recognition to be given to the multiple ways in which the conduct may violate sexual autonomy.

2.5.2 Damage to Privacy and Reputational Harm

Extortion has the potential to cause great damage to one's reputation. Although often treated academically as a financial offence,[177] "in practice many prosecutions concern the betrayal or threatened revelation of sexual secrets, so the rationale of the offence may also include the protection of certain forms of privacy".[178]

Given the ways in which online sexual extortion has developed, far more opportunities exist to obtain sensitive information than previously, and risks to one's privacy and reputation are consequently greater. Even where the perpetrator's motive is primarily sexual or financial, this still raises the question of whether there is incidental damage to privacy and reputation, despite not being the perpetrator's intention. This section will set out how online sexual extortion threatens these interests.

2.5.2(a) Privacy

Interference with an individual's private life is a clear wrong recognised in law.[179] However, this is rarely protected by criminal law,[180] and is more often regulated by civil law[181] or through human rights mechanisms.[182] Yet at its root, one rationale for an extortion offence can be viewed as the protection of one's privacy.

In relation to online sexual extortion, three distinct wrongs are possible. The first is unlawful obtaining of private data relating to the victim (e.g. images; videos; information regarding sexual behaviour or sexuality; passwords; control of online accounts). As set out

[177] See the discussion in Gordon, *Criminal Law* para 28.01.
[178] Horder, *Principles* (n.151) 410; J Herring, *Criminal Law: Text, Cases, and Materials*, 3rd edn (2008) 615.
[179] European Convention on Human Rights and Fundamental Freedoms, Article 8.
[180] J Blackie and J Chalmers, "Mixing and matching in Scottish delict and crime", in M Dyson (ed), *Comparing Tort and Crime* (2015) 271 at 294.
[181] Primarily through an action for breach of privacy or confidentiality.
[182] Human Rights Act 1998 s.7(1).

earlier, this would occur where the perpetrator either obtains personal data through establishing communication or hacking.[183] The second wrong is where the victim's own information is used against them. This may be done to - among other things - coerce the victim into engaging in sexual acts, providing money, or supplying further personal material. It is this activity that is most relevant in terms of online sexual extortion, with this coercion being the core wrong of any act of extortion. The third wrong is that the victim's data may be disclosed if they do meet the perpetrator's demands. For the victim there may consequently be three harms experienced: the initial loss of control over their own data, the coercive use of that data against them, and the ultimate disclosure of that data. Thus, in addition to being characterised as a species of sexual violence, it has also been described as a "form of data breach"[184] whereby an individual loses control over their data with the result that it is used as a means of coercing them into satisfying the perpetrator's desires.

2.5.2(b) Reputation

Similarly, while certain reputational harms may be compensated through an action for defamation, criminal law generally does little to protect this interest. Extortion can be viewed as an exception to this general principle. This is consistent with Hepworth's threefold classification of blackmail, with one category being "where the threat is the revealing to the wider public or a select audience potentially damaging information to one's reputation".[185] Moreover, technology affords opportunities for reputational harm to be brought about in different ways. For example, it is now possible for perpetrators to create sexual images of victims by techniques such as photoshopping. This was the subject of *R v Breakwell*[186] where the defendant used photoshopped images of the victim as a tool with which to extort real sexual images from them. The defendant threatened to publish the photoshopped images unless this demand was met.

As a necessary component of online sexual extortion is a degree of sexual misconduct, there is the potential for the level of harm caused by this conduct to be of a far greater magnitude than in other cases. It has been suggested that this is "[b]ecause there are thoughts

[183] See above at 1.3.3(a) and 1.3.3(c).
[184] Wittes at (n.15) 947.
[185] Hepworth, *Blackmail* (n.42) 1.
[186] [2009] EWCA Crim 2998.

and behaviors of ours that we believe should be kept secret from others…we are vulnerable to exposure of these thoughts and actions (and to blackmail)."[187] The damage to one's reputation can therefore be greatly damaging and embarrassing in these cases.

2.5.2(c) 'Virtual Self'

Taking this further, online sexual extortion can have a great impact on an individual's 'virtual self': an individual's persona in the digital sphere. This may include an amalgam of the following: social media accounts, usernames, passwords, media uploaded online and various forms of communication (e.g. posts; tweets; messages; blog entries). Although not an interest recognised by law, damage to one's virtual identity can have far-reaching consequences. An example is the now common practice of employers undertaking checks on potential and existing employees' social media profiles.[188] Individuals can also face challenges in terms of regaining control of social media profiles once they have become compromised or in establishing new virtual identities.

In terms of privacy, violation of this interest may be a result of a perpetrator having access to online accounts containing highly sensitive personal data including photos, messages, and contacts. This may be "more penetrating, pervasive and permanent".[189] Thus, it is necessary that the law can respond to such severe violations of one's privacy in an adequate manner.

2.5.3 Financial Harm

Finally, extortion is commonly regarded as an offence of dishonesty or a financial offence.[190] The motivation is often financial gain whereby the extorter demands monetary

[187] S Lee, "The nature and value of privacy", in A Cudd and M Navin (eds), *Core Concepts and Contemporary Issues in Privacy* (2018) 47 at 53.
[188] 70% of employers have checked the social media accounts of prospective employees. This figure is 48% in respect of existing employees: (Career Builder, 2017 survey) *https://www.careerbuilder.com/advice/social-media-survey-2017*
[189] W L Robinson, "Digitizing privacy", in Cudd and Navin, *Privacy* (n.187) at 189.
[190] See its treatment in leading criminal law textbooks such as Ormerod & Laird, *Criminal Law* (n.1); Gordon, *Criminal Law*. See also the inclusion of a chapter on blackmail in D Ormerod and D Williams, *Smith's Law on Theft*, 9th ed (2007) 329.

payment on the threat of harm.[191] However, there is no requirement for this under Scots law[192] and while this motive is present in many cases (particularly among organised crime groups) this tends not to be offenders' primary motivation. Although much has been written on the financial motivations of criminal behaviour such as sex trafficking,[193] little consideration has been given to this aspect in respect of online sexual extortion. However, this has received some media attention with reports of organised crime groups operating in (among other countries) Morocco, the Ivory Coast and the Philippines targeting young men in the UK.[194] This has been acknowledged by the NCA who view online sexual extortion as a low-risk way of overseas criminal groups making money.[195] The suicide of Scottish teenager, Daniel Perry, highlights the problems of online groups acting from abroad on an industrial scale. Following this incident, law enforcement agencies were able to identify and dismantle an enterprise in the Philippines. The conduct has been characterised in Asia as comprising "complex operations that involve people across cultures and nations working together to effectively run a very lucrative business"[196] and the organised nature of such operations has resulted in them being compared to call-centres.[197] This has likewise been recognised as an area of great concern across Europe with it being observed that a future retail market for child sexual extortion media is a strong possibility.[198] For those participating in remote sexual extortion from other jurisdictions, this can be viewed as "an opportunity for gaining additional revenue".[199] There is a link between the conduct and pornography. Where an individual is coerced into performing future sex acts as a means of obtaining further intimate images, this must be considered as part of a much larger picture. This represents a very different type of offending from that involving people known to the victim, such as revenge-motivated sexual extortion by former partners or coercive control.

However, that is not to say that financial motivations do not exist among perpetrators acting within this jurisdiction and on a much smaller scale. Examples of this can be seen in *HM*

---

[191] C N Stoddart, "Extortion, corruption and related offences", in *The Laws of Scotland: Stair Memorial Encyclopaedia*, Reissue (2005) para 351.
[192] *Rae v Donnelly* 1982 SCCR 148. See 3.2.1.
[193] For example, see: S Drew, *Human Trafficking - Human Rights: Law and Practice* (2009); M J Guia (ed), *The Illegal Business of Human Trafficking* (2015).
[194] N Massey, "Sextortion: rise in blackmail-related suicides over sexual images shared online", The Independent, (30 Nov 2016). Available at: *http://www.independent.co.uk/news/uk/home-news/sextortion-rise-suicides-blackmailing-sexual-images-sharing-social-media-a7446776.html*
[195] *http://www.nationalcrimeagency.gov.uk/crime-threats/kidnap-and-extortion/sextortion*
[196] Trend Micro Report, "Sextortion in the Far East" (2015) at 12. Available at: *http://www.trendmicro.com.ru/cloud-content/us/pdfs/securityintelligence/white-papers/wp-sextortion-in-the-far-east.pdf*
[197] Europol, *IOCTA* (n.128) at 35.
[198] Europol, *Online sexual coercion* (n.21) at 11.
[199] ibid.

Advocate v Hunter where the perpetrator gained £1,700 from sexual extortion,[200] and in *R v Egege* where £300 was demanded from the victim.[201] While not necessarily posing the greatest threat to victims of online sexual extortion, as with traditional extortion, it is important to recognise that financial harm may occur particularly where targeted by overseas crime groups.

To summarise, this chapter has firstly mapped the problem of online sexual extortion in Scotland, journeying through literature, statistical data and media coverage. It was found that little focus is paid to the issue in the literature, and that under-reporting and difficulties in recording the conduct represent significant challenges to assessing the level of the threat. Despite this, media coverage has raised awareness amongst law enforcement agencies and the wider public, resulting in some promotional campaigns.

In terms of harms, it has been shown that the "online" element of the conduct has changed how extortion may be perpetrated and that those factors examined above allow this offending to be carried out in a far more serious and pervasive manner. This has a severe impact on harms. While sexual harm is the most prominent of these and the conduct should be clearly categorised as a 'sexual offence', we must not lose sight of additional violations of privacy, reputation and financial interests.

[200] *HM Advocate v Joshua Hunter*, sentencing statement published on Judiciary of Scotland website per Lady Scott. Available at: *http://www.scotland-judiciary.org.uk/8/2057/HMA-v-Joshua-Hunter*
[201] *Egege* (n.155).

3 ASSESSING THE CURRENT LEGAL FRAMEWORK

As noted earlier, there is no discrete offence of online sexual extortion under Scots law. However, as the conduct involves a number of elements of potentially criminal conduct, liability may arise in respect of certain existing offences. The first aim of this chapter is to set out which offences under Scots law might impose liability. Building on this, the chapter will assess the effectiveness of these offences by questioning whether they are appropriate to tackle online sexual extortion. It will be argued that while there are a range of offences with sufficient breath to impose liability in most circumstances, there are limitations in terms of adequately capturing the nature and magnitude of the wrongs.

Offences capturing the conduct come from various branches of the criminal law. Most have been around much longer than online sexual extortion. Lawmakers could not have envisaged that such offences would be dealing with this type of conduct. The lack of a specific offence of sexual extortion in any part of the UK means that law enforcement agencies have had to use an array of offences in prosecuting perpetrators, including extortion and causing another to engage in sexual activity.[1] In the US, offences relating to child pornography, computer hacking, and stalking have similarly been cited as relevant.[2] However, although these offences may offer some means of redress, difficulties can arise in convincing prosecutors that existing offences can be used in such circumstances.[3] This is because the offences may not obviously map onto the conduct reported nor the interests harmed.

As discussed in the previous chapter, the fact that the criminal conduct and harms experienced by victims often straddle different areas of the criminal law makes it more difficult to identify adequate responses. This also makes it more challenging to conceptually place where online sexual extortion lies in the field of criminal law. This is a recurring issue when it comes to online sexual offending more generally and this lack of meaningful understanding as to the conceptualisation of the range of behaviours has inhibited the development of suitable and effective responses.[4] This chapter will address this problem by

[1] C McGlynn, E Rackley and R Houghton, "Beyond 'revenge porn': the continuum of image-based sexual abuse" (2017) 25 Feminist Legal Studies 25 at 35.
[2] B Wittes, C Poplin, Q Jurecic and C Spera, Sextortion: cybersecurity, teenagers, and remote sexual assault (Center for Technology Innovation at Brookings, 2016) at 4, 5.
[3] McGlynn et al (n.1) at 35.
[4] N Bluett-Boyd, B Fileborn, A Quadara and S Moore, "The role of emerging communication technologies in experiences of sexual violence: a new legal frontier?" (Australian Institute of Family Studies Research Report No.23, 2013) at 11. Available at: *https://aifs.gov.au/publications/role-emerging-communication-technologies-experiences-sexual-violenc*

building on the identification of the harms in Chapter 2 and assessing the offences in terms of how well they protect against these specific harms.

In Scots law there is no formal classification of crimes into groups.[5] However, writers frequently categorise offences according to the interest they appear to threaten.[6] Alldridge explains the importance of this: "unless crimes are classified appropriately – that is, unless the exact wrong can be identified…it will be impossible to label, to compare, or to sentence justifiably".[7] This is supported in a leading Scots criminal law textbook, which remarks that "grouping offences into categories assists in articulating what it is about the prohibited behaviour that is reprehensible".[8] Why is this relevant? Because how we choose to categorise a species of conduct can have consequences in terms of the value the criminal law places on an interest. In this context, it is important to be able to identify the interest that the criminal law protects in cases of online sexual extortion. Only by doing this can effective responses be propounded. It would seem that there are three core interests that it threatens. These are sexual autonomy, personal autonomy (specifically privacy and reputation interests), and property. The evaluation of the current legal framework will accordingly be undertaken by reference to the type of offence being considered. For the purposes of this assessment the relevant offences have been grouped into the following categories: sexual offences, dishonesty offences, and non-fatal non-sexual offences against the person. Following this, a broader evaluation at the end of the chapter will draw on this analysis by identifying overarching problems with the existing law and arguing that these must be remedied in order to improve the criminal law's response to online sexual extortion.

3.1 Sexual Offences

As concluded in the previous chapter, all instances of online sexual extortion must necessarily involve – at least to some extent – violation of an individual's sexual autonomy. Sexual offences is therefore the criminal law branch most likely to afford protection to such

[5] T Jones and I Taggart, *Criminal Law*, 7th edn (2018) para 2-28; A M Cubie, *Scots Criminal Law*, 4th edn (2016) para 1.11.
[6] P Ferguson and C McDiarmid, *Scots Criminal Law: A Critical Analysis*, 2nd edn (2014) para 2.1.3
[7] ibid 101 quoting P Alldridge, "The Public, the Private and the Significance of Payments", in P Alldridge and C Brants (eds), *Personal Autonomy, the Private Sphere and Criminal Law* (2001) 79 at 80.
[8] Ferguson & McDiarmid, *Scots Criminal Law* 101.

victims. This section will begin by setting out the structure of sexual offences in Scots law before providing an analysis of the ways in which online sexual extortion vitiates consent. Following on from this, specific offences will be discussed in order to evaluate how well these offences respond to this conduct.

What is the purpose of sexual offences? Ashworth views this as being "to protect the autonomy of individuals in sexual encounters, ensuring that there are criminal prohibitions to prevent unwanted sexual interference and to criminalise those who culpably interfere with individuals' sexual autonomy".[9] One would think that recent reform of this area in Scotland - resulting in the Sexual Offences (Scotland) Act 2009[10] – would ensure that this jurisdiction is well placed to deal with this type of behaviour. Although there is no specific provision for sexual extortion (online or otherwise) in the 2009 Act, there are offences that can be used in prosecuting it. These are sexual coercion offences, indecent communication, voyeurism and sexual exposure. However, other sexual offences not contained in the 2009 Act such as grooming and pornography offences merit some discussion.

It will be argued in this section that although existing sexual offences will evidently be important in capturing certain cases of online sexual extortion, no single offence truly captures the harms experienced by victims, nor sufficiently deals with the potential multitude of these harms.

3.1.1 Sexual Offences (Scotland) Act 2009

In assessing how effectively the 2009 Act deals with online sexual extortion, it is firstly important to consider the purpose of the sexual offences reform. The Act aims to provide a set of codified rules designed to cover a wide range of offending.[11] Central to these offences is the protection of sexual autonomy.[12] The relevant offences are framed around the notion of consent and it is the absence of consent which makes the proscribed acts criminal. As a

[9] A Ashworth and J Horder, *Principles of Criminal Law*, 7th ed (2013) 338.
[10] See Report on *Rape and Other Sexual Offences* (Scot Law Com No 209, 2007) for background to the reform of sexual offences in Scotland.
[11] But note the remark in G H Gordon, *Criminal Law of Scotland*: Vol 2, 4th edn, by J Chalmers and F Leverick (2016) para 41.01 that the 2009 Act "is not a comprehensive code of *all* offences related to sexual behaviour" (emphasis added).
[12] Report on *Rape and Other Sexual Offences* para 1.25.

result, the victim's lack of consent is part of the *actus reus* of each offence, with this disregard for the victim's autonomy being the defining element of these offences.[13] The interaction between the specific consent provisions found in the 2009 Act and online sexual extortion will be assessed below, specifically regarding those circumstances where there can be no consent. These factual circumstances are contained in section 13 of the Act and it is stated that consent is absent in such instances.[14] Consent itself is defined in the 2009 Act by reference to "free agreement"[15] and where a case falls outwith the factual situations in section 13, the presence of consent is determined by asking whether free agreement was present. It will be argued that coercion in the form of extortion will vitiate consent in most online sexual extortion cases and that although the provisions in section 13 are relevant, ultimately liability for sexual offences under the 2009 Act will arise as there will be no free agreement.

Finally, it is worth reiterating that in some cases of online sexual extortion, the question of consent will be of less significance as the victim may be a child. However, this is subject to the caveat that it may still be necessary to examine consent where the child is an older child as this can have an impact in terms of the offence the accused may be charged with.[16]

3.1.1(a) Consent and Sexual Extortion

There are two specific instances where consent is deemed to be absent that are relevant for the purposes of this research. Firstly, where the sexual conduct took place as a result of deception on the part of the perpetrator.[17] Secondly, where it occurred as a result of threats of violence.[18] In both instances there can be no consent. The significance of each of these negative indicators will now be discussed in turn.

[13] ibid para 2.18-2.19 for background to sexual offence reform in Scotland.
[14] Sexual Offences (Scotland) Act 2009 s.13(1).
[15] ibid s.12.
[16] See 1.3.2.
[17] 2009 Act s.13(2)(d).
[18] ibid s.13(2)(b).

3.1.1.(a)(i) Deception

In a sexual context, fraudulent behaviour on the part of the perpetrator may result in liability for a sexual offence, as the fraudulent act will have the effect of negating consent.[19] However, in terms of the legislation, consent is only deemed to be absent where deception is as to the "nature or purpose" of the sexual conduct.[20] Beyond this, whether deception by the perpetrator negates consent is determined by reference to the definition of consent as "free agreement".[21] It will be for the court to find whether this is absent based on the facts.

In terms of the operation of the rule under section 13(2)(d), there is no authority. There are, however, decisions from other jurisdictions with a similarly worded provision. From these decisions, this provision is to be narrowly construed. Where deception in question is as to a collateral matter then this will generally not negate consent.[22] In one Australian case a rape conviction was quashed where the defendant caused a woman to have sexual intercourse with him by pretending they were married to one another.[23] Likewise, in *Clarence* it was stated by Wills J that "consent obtained by fraud is no consent at all is not true as a general proposition either in fact or in law".[24] As a result, fraud will vitiate consent "only in the most exceptional cases".[25]

This issue recently came before the courts in England in two appeal cases concerning the equivalent provision in the 2003 Act.[26] The first was *R v Devonald*.[27] This was an appeal against conviction after the appellant had initially pleaded guilty to the offence of causing a person to engage in sexual activity. Following the breakdown of a relationship between the appellant's daughter and her boyfriend, the 37 year old appellant began online communications with the boyfriend, assuming the identity of a 20 year old female. These communications became sexual and the appellant encouraged the complainer to masturbate in front of a webcam. The Crown argued that there was clearly deception in these circumstances. Had the complainer known that the 20 year old female he was

[19] ibid Act s.13(2)(d).
[20] ibid.
[21] ibid s.12.
[22] *R v Papadimitropolous* (1957) 98 CLR 249; see also the English case of *R v Linekar* [1995] 3 All ER 69 for a similar approach.
[23] ibid *Papadimitropolous*.
[24] *R v Clarence* (1888) 22 QBD 23.
[25] G Syrota, "Rape: when does fraud vitiate consent?" (1995) 25 Western Australian Law Review 334 at 335
[26] 2003 Act s.76(2)(a).
[27] [2008] EWCA Crim 527.

communicating with was his former girlfriend's father, he would not have engaged in this sexual activity.[28] It was therefore the Crown's position that the appellant's deception vitiated any consent and went to the purpose of the relevant act.[29] This was because the complainer believed he was consenting to sexual acts for the sexual gratification of a 20 year old female, rather than the appellant, whose motivation was to "teach him a lesson" by later exposing the recorded acts.[30] Thus, although the nature of the activity remained sexual – regardless of deception – that the purpose was significantly different was sufficient for the Court of Appeal to find there was deception as to the purpose of the sexual act.[31] The result was that there could not have been consent[32] and that the appellant was guilty of causing the complainer to engage in sexual activity without consent.

However, this decision was later criticised in *R v Bingham*[33] where the Court of Appeal reviewed the operation of this provision. The appellant challenged seven convictions for causing a person to engage in sexual activity without consent. The appeal was based on the Crown's position at trial. The Crown had stated that the appellant's purpose had been sexual gratification, and as such, the appellant argued that assuming the complainer had known this was his purpose, there was consequently no deception as to purpose.[34] The facts are that the appellant had assumed two false identities as a means of making his girlfriend send intimate images and carry out penetrative sexual acts over a webcam. Although these facts were not in dispute, the appellant maintained that at all times he believed the complainer was consenting, but his motive was to teach her "to stand up for herself and say no to people".[35] The Crown's position was that the appellant was likely motivated by sexual gratification accompanied by a possible "power trip".[36] They argued that the deception went to the purpose of the sexual acts under section 76(2)(a), relying on the decision in *Devonald*.[37] The defence, on the other hand, sought to rely on the decision in *R v Jheeta*.[38] In this case the complainer was deceived by an elaborate fantasy created by her partner, the appellant. After receiving death threats the complainer instructed the appellant to inform the police. The appellant thereafter posed as police officers and sent the complainer a number of text

[28] *Devonald* at para 3.
[29] ibid at para 6.
[30] ibid at para 3.
[31] ibid at para 9.
[32] 2003 Act s.76(2)(a).
[33] [2013] EWCA Crim 823.
[34] ibid at para 17.
[35] ibid at para 6.
[36] ibid.
[37] ibid at para 9.
[38] [2007] EWCA Crim 1699.

messages. These pressured the complainer into maintaining a sexual relationship with the appellant and she continued to engage in sexual activity. The appellant's original conviction was quashed on appeal. It was held that the complainer had not been deceived as to the "nature or purpose" of the sexual intercourse, but rather was "deceived as to the situation she found herself in".[39] The court in *Bingham* was more persuaded by the reasoning in *Jheeta*. They found that the complainer in *Bingham* had knowledge of what she was being instructed to do; by performing sexual acts in front of a webcam she must have known that the motive of the appellant was, at least to some extent, sexual gratification.[40] Thus, although the court acknowledged the unpleasant nature of the deception, they nevertheless held that it did not go to the purpose of the sexual activity itself, but rather to the circumstances surrounding the activity.[41]

This decision must also be considered in the context of the statutory provision itself. Where a provision provides a conclusive presumption that consent is absent (or is simply indicative of a lack of consent) then this must be narrowly construed on the basis that it has the effect of restricting a defendant's ability to present a defence.[42] Furthermore, there is still the possibility of the general consent rule[43] (free agreement) being engaged by the jury.[44] This was confirmed in *Bingham* where the judge criticised the Crown's reliance on the conclusive presumption and stated "[i]f the complainant only complied because she was being blackmailed, the prosecution might argue forcefully she did not agree by choice".[45] The Crown, in relying solely on section 76, failed to lead evidence on the more general question of whether there was free agreement between the parties. Had they done this then a conviction might have been secured.

It is therefore likely in light of the case law that the conclusive presumption in section 13(2)(d) in Scots law would be applied restrictively. The relevance for online sexual extortion cases is that there would have to be deception as to the nature or purpose of the sexual act in question; mere deception as to personal characteristics or identity will not be sufficient for the purposes of section 13(2)(d).[46] As a number of online sexual extortion cases

[39] ibid at para 28 per Sir Igor Judge.
[40] *Bingham* at para 22.
[41] ibid at para 21.
[42] ibid at para 23. See also P Rook and R Ward, *Rook & Ward on Sexual Offences: Law and Practice*, 5th ed (2016) para 1.313.
[43] 2003 Act s.74. For the equivalent provision under Scots law see: 2009 Act s.12.
[44] Gordon, *Criminal Law* para 38.10; Rook & Ward, *Sexual Offences* para 1.319.
[45] *Bingham* at para 24 per Hallett LJ.
[46] Except where the deception is as to the identity of an individual personally known to the complainer. See 2009 Act s.13(2)(d).

are more in line with the facts in *Bingham*, it is less likely that section 13(2)(d) would be engaged. In the majority of cases the victims will not be deceived as to the nature or purpose of a sexual act and will likely share the perpetrator's purpose of sexual gratification. However, it is possible that where the perpetrator has an altogether different purpose that the provision may become relevant. In all other cases, the question would be whether there was free agreement.

3.1.1(a)(ii) Violence and Threats of Violence

The other situation relevant to online sexual extortion where consent is deemed absent is where the victim submits to sexual activity by reason of threats of violence made against themselves or another individual.[47] The key question here is one of causation: there must be a causal link between threats against the victim and the agreement or submission to the sexual conduct in question.[48] This requirement may make securing a conviction difficult.[49] Causation may be harder to establish where the victim has had no physical contact with the perpetrator. Furthermore, this specific provision is limited as it only covers threats of violence and not those cases where the threat is the exposure of sexual material. It would, however, ensure that cases such as those referred to in the previous chapter where the threat is of sexual harm would be included, assuming this threat caused the victim's agreement or submission to the sexual conduct. Despite this, as with deception, in most cases the issue of consent will fall to be determined according to the general consent definition.[50]

To put the consent provisions in context, it is necessary to consider briefly some of the relevant sexual offences found in the 2009 Act and to assess their suitability in capturing instances of online sexual extortion.

[47] 2009 Act s.13(2)(b).
[48] Report on *Rape and Other Sexual Offences* (n.10) para 2.66ff
[49] Gordon, *Criminal Law* para 38.08.
[50] 2009 Act s.12.

3.1.1(b) Sexual Coercion

One of the most obvious offences in the 2009 Act that captures online sexual extortion is sexual coercion.[51] This makes it an offence for a person, A, to intentionally cause another person, B, to participate in sexual activity where the following two conditions are met: that B does not consent to participate in the sexual activity and where A has no reasonable belief that B consents to participating in that activity.[52] It is also necessary to prove that the accused acted for the purposes of obtaining sexual gratification, or to humiliate, distress or alarm the victim.[53]

Despite the name of the offence, there is no requirement of 'coercion' in a physical sense. The offence is instead based around the victim's lack of consent. As such, the SLC states that the offence is broad and can be committed in a number of ways.[54] The offence seeks to expressly criminalise conduct where the perpetrator causes the victim to engage in sexual conduct that may not physically involve the perpetrator. This could be conduct that would not fall within the scope of sexual assault. The offence really turns on the question of what is meant by 'causing'? A discussion of the equivalent English offence[55] suggests that this could be either by "explicit or implicit threats, or by use of a position of authority or dominance (simply by speaking words)".[56] Where an individual engages in sexual activity that they otherwise would not have without the use of coercion or threats then liability would arise in respect of this offence.

In addition to the offence of causing an individual to participate in sexual activity under section 4, there are also two related 'coercion offences': causing an individual to be present during sexual activity,[57] or to look at a sexual image.[58] The rationale for both offences appears the same: i.e. that being forced to watch sexual activity or to view sexual activity is just as much a violation of sexual autonomy as being forced to participate in sexual activity.[59]

[51] ibid s.4.
[52] ibid s.4(1).
[53] Ferguson & McDiarmid, *Scots Criminal Law* (n.6) para 11.5.1.
[54] Report on *Rape and Other Sexual Offences* (n.10) para 3.48.
[55] 2003 Act s.4.
[56] Ashworth and Horder, *Principles* (n.9) 353.
[57] 2009 Act s.5(1).
[58] ibid s.6(1).
[59] Report on *Rape and Other Sexual Offences* (n.10) para 3.55.

These offences have the benefit of reflecting the violation of a victim's sexual autonomy. The primary offence of causing an individual to engage in sexual activity suitably and clearly labels one aspect of wrongdoing in online sexual extortion cases: where a victim's will is overcome as a result of coercion or threats and they are consequently made to engage in sexual activity without giving valid consent. However, this is just one element of online sexual extortion. The offence does not capture additional harms a victim may suffer, including damage to privacy, reputation and economic interests. Nor does the offence necessarily capture the continuous and prolonged coercion that an individual may have to endure. It simply recognises and addresses the wrong at the moment the victim engages in sexual activity[60] without consent. The wrongdoing in many online sexual extortion cases is much broader than this and ought to be reflected in terms of the criminal liability imposed.

3.1.1(c) Indecent Communication

Another offence that would capture conduct in online sexual extortion cases is that of indecent communication.[61] As will be discussed below, other communications offences aimed at tackling threatening and abusive behaviour may also be relevant when it comes to online sexual extortion. However, this offence specifically applies where the communication is sexual[62] and is sent or directed to the victim without their consent.[63] The *mens rea* is that the communication was directed with the intention of either obtaining sexual gratification,[64] or humiliating, distressing or alarming the victim,[65] and there was no reasonable belief that the victim consented.[66] This applies both to written and verbal sexual communications that are sent or directed by whatever means.[67] There are equivalent provisions that apply where the perpetrator causes an individual to see or hear (rather than sends or directs) a written or verbal sexual communication.[68]

[60] Or in the case of the related offences is present during sexual activity or views a sexual image
[61] 2009 Act s.7(1).
[62] ibid.
[63] ibid s.7(1)(a).
[64] ibid s.7(3)(a).
[65] ibid s.7(3)(b).
[66] ibid s.7(1)(b).
[67] ibid s.7(1).
[68] ibid s.7(2).

What are the rationales for these offences? As with a number of other offences in Part 1 of the 2009 Act, the victim's lack of consent is a core element of the offences and forms part of the *actus reus*. Thus, there can be no indecent communication unless the victim does not consent to the communication in question.

There are two ways in which the offence may be committed in an online sexual extortion case. Firstly, where the victim simply does not consent to communication in question. An example of this can be seen in *Kidd v McGowan*[69] where the accused pled guilty to this offence after threatening to rape two individuals.

Secondly, where the victim is deceived and this deception makes the communications non-consensual. This may where the perpetrator deceives the victim as to their identity or personal characteristics. In such cases it may be that there is no free agreement and that liability would therefore arise for indecent communication.

As discussed in the first chapter, it may be that the perpetrator and victim initially engage in consensual 'sexting' prior to any extortion or coercion on the part of the perpetrator. However, the mere fact that the motive at the time was either to receive sexual material belonging to the victim in order to later use against them, or was entirely innocent and the extortion was only thought of later, does not impact on this conduct. If the materials were acquired consensually at the time then there can be no liability for indecent communication.

3.1.1(d) Voyeurism

Voyeurism criminalises the viewing of another individual engaging in a private act without that individual's consent.[70] The *mens rea* is the intentional viewing with the purpose of obtaining sexual gratification or causing humiliation, distress or alarm to the victim.[71] A private act is defined as being one which in the circumstances would reasonably be expected to provide privacy.[72] Additionally, the complainer's genitals, buttocks or breasts must be either exposed or covered with underwear, or they must be engaging in a sexual act "that is not of the kind ordinarily done in public".[73] The legislation further provides that the offence

[69] [2012] HCJAC 163.
[70] 2009 Act s.9.
[71] ibid s.9(6).
[72] ibid s.10(1).
[73] ibid.

can be committed electronically and by use of recording equipment or a webcam,[74] thereby encompassing online wrongdoing.

Voyeurism may therefore capture conduct at early stages, where the perpetrator is watching their victim without consent, and specifically where a perpetrator remotely accesses their victim's technological devices. However, it fails to really get to grips with the more serious elements of online sexual extortion, particularly the coercive or threatening nature of it. It is nevertheless an important offence in tackling what may be considered more as preparatory conduct.

3.1.1(e) Sexual Exposure

The final relevant offence under the 2009 Act – and somewhat related to the preceding discussion on indecent communication – is sexual exposure. For the purposes of this offence, 'exposure' means intentional exposure of "genitals in a sexual manner"[75] without the consent of the victim.[76] This must be done for the purposes of either obtaining sexual gratification[77] or humiliating, distressing or alarming the victim,[78] and without reasonable belief that the victim consents.[79]

As with voyeurism, liability for sexual exposure is only likely to arise in respect of preparatory conduct in online sexual extortion cases. However, in accordance with the typology set out in the first chapter, it may be that the perpetrator commits this offence in order to either build rapport with or disinhibit the victim, or in the hope that the victim may reciprocate this conduct. In the event of the latter, this may be to obtain sexual material of the victim which can then be used as a means of extortion.

[74] ibid s.9(3), (4), (4A), (4B), (5)(a).
[75] ibid s.8(1).
[76] ibid s.8(1)(a).
[77] ibid s.8(2)(a).
[78] ibid s.8(2)(b).
[79] ibid s.8(1)(b).

3.1.2 Other Sexual Offences

There are other sexual offences that are not contained in the 2009 Act and liability may arise in respect of these offences in cases of online sexual extortion. These are grooming, and pornography offences.

3.1.2(a) Grooming

Provision for grooming is found in the Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005[80] and the primary offence is that of meeting a child following certain preliminary contact.[81] The rationale for such an offence was to allow for early intervention by police officers to prevent the escalation of sexual conduct by sexual offenders.[82] As with the introduction of such an offence in England,[83] this can be viewed as a response to the grooming of children through electronic communications. Notwithstanding that this offence seeks to target preparatory conduct[84] – there is no requirement of *actual* sexual abuse of children for liability to arise – the offence is severe with a maximum sentence of up to as much as 10 years' imprisonment on indictment.[85]

For liability to arise the first requirement is that a person, A, intentionally meets B, travels in any part of the world with the intention of meeting B, or makes arrangements in any part of the world to meet B,[86] with the intention of engaging in unlawful sexual activity involving B or in the presence of B, during or after the meeting and in any part of the world.[87] The second requirement is that B is aged under 16[88] and A does not reasonably believe that B is aged 16 or over.[89]

In terms of suitably capturing instances of online sexual extortion, this offence has several limitations. Firstly, it is only relevant in cases where the victim is under the age of 16.

---

[80] Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005.
[81] ibid s.1.
[82] Gordon, *Criminal Law* para 41.25.
[83] 2003 Act s.15.
[84] S Pegg and A Davies, *Sexual Offences: Law and Context* (2016) 90.
[85] 2005 Act s.4.
[86] ibid s.1(a).
[87] ibid s.1(b).
[88] ibid s.1(c)(i).
[89] ibid s.1(d).

Secondly, the offence additionally requires that the perpetrator must have met or communicated with the victim on at least one earlier occasion. This means that it will not apply to remote access cases, but only to instances where the perpetrator has communicated with the victim and developed a relationship. It may also be that owing to this requirement, the offence would be more likely to apply to those cases where there is a pre-existing relationship between the parties with this providing opportunity for such conduct to occur.

The third limitation is that it must be proved that the person communicating with the child only did so with the intention of meeting them in person. In 'purely cyber' cases where the perpetrator is engaging solely in online abuse, it is unlikely that they will possess this intention. Without this intention no liability for this offence will arise.

However, the term 'blackmail grooming'[90] has been used in respect of conduct where child victims have been coerced into meeting perpetrators. An example of this in one Scottish case of online sexual extortion where the accused booked a hotel room and this formed part of his demand that he would only delete sexual images of the victim if she met him there and engaged in sexual activity.[91]

As a result, grooming is only of relevance where the offender plans to move from the online sphere to the physical world,[92] but this may capture some cases of online sexual extortion where part of the perpetrator's demand includes meeting in person for the purposes of sexual activity.

3.1.2(b) Pornography Offences

Online sexual extortion can be viewed in some situations as a means of creating pornographic material[93] and this may be the wider motive of the perpetrator in engaging in extortion.[94] As with grooming, for liability to arise the victim must be a child (or at the very least that there will be some involvement of a child).

---

[90] Bluett-Boyd et al (n.4) at 32.
[91] *HM Advocate v Andrew McBride*, sentencing statement published on Judiciary of Scotland website per Lord Turnbull. Available at: *http://www.scotland-judiciary.org.uk/8/1360/HMA-v-ANDREW-MCBRIDE*.
[92] K Veli, "Sexual extortion of children in cyberspace" (2016) 10 International Journal of Cyber Criminology 110 at 112.
[93] See 2.5.3.
[94] Europol European Cybercrime Centre, *Online sexual coercion and extortion as a form of crime affecting children - Law Enforcement Perspective* (May 2017) at 11. Available at:

The Civic Government (Scotland) Act 1982 criminalises a number of different activities relating to indecent photographs of children.[95] A child is defined for these purposes as someone under the age of 18,[96] subject to the exceptions contained in section 52B of the same Act relating to images of 16 and 17 year olds.[97] This goes some way in attempting to protect young people who may be vulnerable to targeted online sexual offending. It is additionally necessary that there is a photograph, the definition of which includes a film[98] (or any form of video-recording).[99] The main conduct that the legislation criminalises is the possession of indecent images of children,[100] as well as the taking,[101] distribution,[102] showing,[103] and publication[104] of such images.

This legislation is useful where a child is coerced into creating sexual material, or where the perpetrator carries through with threats to show, distribute or publish this material. However, these offences are limited to these circumstances and although very serious, fail to capture additional wrongs present in online sexual extortion cases such as the prolonged control and sexual coercion of a child victim.

3.2 Offences of Dishonesty

As set out earlier, a core element of online sexual extortion is often the deception and dishonesty employed by perpetrators in establishing contact with potential victims. It is likely that the offences of extortion or fraud may be committed in these circumstances.

https://www.europol.europa.eu/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf

[95] Civic Government (Scotland) Act 1982 s.52.

[96] ibid s.52(2).

[97] ibid s.52B. The main exception is where the photograph is of a child aged 16 or over and that child is either married, in a civil partnership, or in an established relationship with the accused, and consented to the photograph being taken or made.

[98] ibid s.52(8)(a).

[99] ibid s.52(8)(d).

[100] ibid s.52A(1). There is a separate offence of possessing an image with a view to it being distributed or shown to others (s.52(1)(c)).

[101] ibid s.52(1)(a).

[102] ibid s.52(1)(b).

[103] ibid.

[104] ibid s.52(1)(d).

3.2.1 Extortion

An assessment of offences capturing online sexual extortion must include discussion of one of the conduct's fundamental elements: extortion. Liability for extortion will arise where the perpetrator goes beyond mere deception or coercion and has progressed to a demand backed by a threat.

In Scots law extortion is defined as being "the crime of obtaining money or any other advantage by threats, often known in non-technical language as blackmail".[105] This is of greater utility than the related English law offence of blackmail. This is because extortion under Scots law does not seek to restrict the nature of the demand issued by the perpetrator. This stems from the writings of Hume who wrote that extortion may occur where there is a threat against an individual "unless something shall be done, or shall be desisted from",[106] without limiting this demand to the payment of money. This is in contrast to blackmail, where there must be a demand relating to a gain of money or other property, or for there to be a loss to the victim of money or other property.[107] While blackmail is therefore commonly viewed as an offence against property,[108] extortion can be categorised more as an offence of dishonesty, or in some instances as an offence against the person given its potential to restrict one's liberty.[109]

Extortion can consequently take a number of forms. As a result, much has been written on its basis and justification in the criminal law. Much of the justification is based on the coercive effect on the victim, whose liberty is restricted by demands and corresponding threats. This is regardless of whether the threat or demand is legitimate.[110] An example of this was in *Rae v Donnelly*[111] where the demand was that the victim acted in a certain way (in this instance that they dropped a case of unfair dismissal against the perpetrator's company) and the threat was the exposure of an extra-marital affair. Thus, the parameters of

[105] Gordon, *Criminal Law* para 28.01.
[106] D Hume, *Commentaries on the Law of Scotland, Respecting Crimes* (1797) I, 439.
[107] Theft Act 1968, s.34(2) ("'gain' or 'loss' are to be construed as extending only to gain or loss in money or other property but as extending to any such gain or loss whether temporary or permanent").
[108] D Ormerod and K Laird, *Smith and Hogan's Criminal Law*, 14th ed (2015) 1067; Horder, *Principles* (n.9) 409.
[109] Gordon, *Criminal Law* para 28.01, citing P H Robinson, *Criminal Law* (1997) para.14.5
[110] There is no requirement under Scots law that the threat or demand be wrongful. This has created what has been termed as the "blackmail paradox". The literature on this is vast. See: Ormerod & Laird, *Criminal Law* (n.108) 1070-71 for an overview.
[111] 1982 SCCR 148.

the offence are very wide. In *Black v Carmichael*,[112] Lord Justice-General Hope asserted that "it is extortion to seek by such means to obtain money or some other advantage to which the accused has no right at all".[113] It is submitted that the phrase "some other advantage" would be sufficiently broad so as to cover sexual gratification, despite there being no authority on this point.[114] However, in some cases it may not be clear what advantage the perpetrator will be gaining. An example would be where the perpetrator demands that the victim performs a live sexual act under the threat of exposing a prior video of them engaging in such an act. If the perpetrator is not receiving sexual gratification then is there a recognisable gain? As such it may be more appropriate to turn our attention towards the loss (if any) sustained by the victim. It is clear that a gain is not necessarily required for liability to arise. Where the victim suffers a loss, this may fall within the scope of extortion. It was stated in *Silverstein v HM Advocate*[115] that "[w]here the pressure consists in creating in the victim fear that, unless he yields, his position will be altered for the worse, it is criminal unless the pressure sought to be exerted is recognised by the law as legitimate".[116] Although the loss may not be patrimonial, the victim will have suffered a violation to their sexual autonomy. This violation will be clear if, for example, they are ordered to perform a sexual act under the looming threat of their privacy and autonomy being further infringed by the possible dissemination of images or video recordings of them.

As expressed in the previous chapter, the key is that offences used in response to online sexual extortion recognise the breach of sexual autonomy suffered by victims. This is irrespective of whether the breach is from being coerced into participating in sexual acts or activity, or whether it is through threats to reveal sexual material relating to the victim. Although a very serious offence, what extortion lacks in cases resulting in violation of one's sexual autonomy is to send a message regarding the nature of the wrong committed by the perpetrator against the victim. This is to some extent linked to the issue of labelling. It is not to say that extortion is not regarded a sufficiently serious offence (for it is). However, it fails to convey both the culpability of the offender (who may have caused long-lasting and permanent physical or psychological harm to their victim) or the nature of harm suffered by the victim, who may have experienced a serious violation of their sexual autonomy.

---

[112] 1992 SLT 897.
[113] ibid per Lord Justice-General Hope at 900.
[114] It is nevertheless stated in Gordon, *Criminal Law* para 28.04 that "it would accordingly be extortion for A to induce a woman to have sexual intercourse with him by threatening her that unless she did so he would tell her husband of her adultery with B".
[115] 1949 JC 160.
[116] ibid per Lord Justice-Clerk Thomson at 163.

3.2.2 Fraud

As noted earlier, many online sexual extortion cases involve an element of deceit. In these instances it is likely that the perpetrator will have committed the offence of fraud, even before any threats are issued or sexual misconduct has occurred. Fraud has a very broad ambit under Scots law.[117] Although more associated with financial crime, there is no reason why the offence cannot cover fraudulent conduct in this context. As with extortion, Scots law benefits from a broader concept of fraud than the equivalent English statutory offence, which requires a gain or loss of money or other property.[118]

This chapter has already examined the link between fraud and sexual offences in terms of consent. However, as stated above, the majority of cases will fall to be determined according to the general definition of consent as 'free agreement',[119] rather than the specific consent provision relating to fraud as to the nature or purpose of the sexual act.[120]

Despite this, the common law offence may fill gaps where a sexual offence cannot be made out by prosecutors or where there is insufficient evidence to charge the accused with extortion. Notwithstanding this, in *HM Advocate v McBride*, the accused was charged with fraud alongside numerous extortion charges, which shows its relevance in practice.[121]

There are three elements to fraud: acting with a false pretence, achieving a definite practical result, and a causal connection between the pretence and result.[122] The first criterion of acting with a false pretence is the act of deception itself and should be easily made out where the perpetrator uses a false identity or otherwise deceives the victim. However, where the victim is aware of the perpetrator's true characteristics, there may be no deception to begin with and therefore no fraud.

The second criterion is bringing about a definite practical result. Would this cover situations where the perpetrator deceives the victim as to their identity or characteristics without seeking financial gain? In *Adcock v Archibald*[123] it was held that pecuniary loss need not be

[117] Gordon, *Criminal Law* para 25.01.
[118] Fraud Act 2006 s.5(2)(a). This is consistent with the Theft Act 1968: see D Ormerod and D Williams, *Smith's Law on Theft*, 9th ed (2007) 135.
[119] 2009 Act s.12.
[120] ibid s.13(2)(d).
[121] *HM Advocate v Andrew McBride* (n.91) per Lord Turnbull.
[122] Gordon, *Criminal Law* para 25.02.
[123] 1925 JC 58.

proved for liability to arise for fraud: "any definite practical result" is sufficient.[124] This means that fraud is committed so long as the victim is deceived into doing "some act he would not otherwise have done, or to become the medium of some unlawful act".[125] On this basis, this would cover a number of acts falling within the scope of online sexual extortion as set out in Chapter 1. This breadth was recently affirmed by the appeal court in *Whyte v HM Advocate*.[126] The court dismissed the appellant's plea to the relevancy that as the pleadings failed to aver any loss, the Crown had not libelled a definite practical result.[127] The appellant contended that the victim "must be shown to be in a worse position than he or she otherwise would have been but for the fraud".[128] However, the court held that the principle in *Adcock* has the advantage of being "clear, objective…[and] sufficiently flexible".[129] The offence of fraud would consequently be committed where there is a "dishonest misrepresentation of fact which is designed to bring about the practical result which eventuates".[130]

Despite its recently confirmed scope, fraud's applicability to cases of online sexual extortion is perhaps of less relevance in light of the above statement that this would now be seen as negating consent and thus constitute a sexual offence under the 2009 Act. Although the conclusive presumption in relation to fraud appears somewhat narrow, a number of cases of online sexual extortion would still raise questions regarding consent by reference to the general definition of consent.[131] In light of this, the relevance of common law fraud to online sexual extortion is therefore likely to be somewhat diminished.

3.3 Non-Fatal Non-Sexual Offences Against the Person

As set out in the previous chapter, online sexual extortion extends beyond sexual and financial harms. Other harms can occur, including infringement of one's right to privacy or damage to reputation. For the purposes of this thesis, these offences have been categorised

[124] ibid at 61 per Lord Justice-General Clyde.
[125] ibid at 61 per Lord Hunter.
[126] 2017 JC 262.
[127] ibid at para 4.
[128] ibid.
[129] ibid at para 15 per Lord Justice-Clerk Dorrian.
[130] ibid at para 16 per Lord Justice-Clerk Dorrian.
[131] 2009 Act s.12.

as "non-fatal non-sexual offences against the person",[132] but could also be referred to as offences infringing liberty or as offences of threatening behaviour.

3.3.1 Threatening Behaviour

The simple act of issuing a threat may in certain circumstances constitute a criminal offence. The law in this area has developed in a very piecemeal fashion with there being historic offences at common law, as well as specific statutory offences. These categories will briefly be considered in turn.

3.3.1(a) Threats at Common Law

Although a threat backed by a demand would in most cases be charged as extortion, threats with nothing more could constitute the common law offence of threatening another individual. There is a distinction at common law between threats that are criminal *per se* and those threats that are only criminal when accompanied by a specific mental element.[133]

At common law various threats are criminal including those to "burn a man's house…to put him to death, or to do him any grievous bodily harm, or to do any serious injury to his property, his fortune, or his reputation".[134] In such cases criminal liability arises at the moment the threat is made and this includes oral or written threats.[135]

The second category is threats that are criminal because of the accompanying intention of the accused. These tend to apply more to limited factual circumstances (such as where a witness is threatened into not giving evidence).[136]

In general, such offences are likely to be of little utility as the core element of online sexual extortion is a threat accompanied by a demand. Bare threats are more relevant in capturing preparatory conduct such as where the perpetrator seeks to intimidate the victim without

[132] J Horder, "Rethinking non-fatal offences against the person" (1994) 14 OJLS 335 at 335.
[133] Gordon, *Criminal Law* para 48.01.
[134] *Jas Miller* (1862) 4 Irv 238 at 244.
[135] Gordon, *Criminal Law* para 48.01.
[136] ibid para 48.02.

making any demand, or where the demand is merely implied and difficulties arise in proving that a demand was communicated to the victim.

3.3.1.(b) Statutory Threats

In addition to the aforementioned common law offences, some statutory provisions criminalise threats. Most relevant here is the broad offence of threatening and abusive behaviour.[137] Key elements of this offence are that the perpetrator, A, behaves in a threatening or abusive manner, that this behaviour would likely cause a reasonable person to suffer fear or alarm, and that A either intends to cause such fear or alarm, or is reckless as to this.[138] The legislation sets out that behaviour can include a single act or course of conduct, and includes communications as well as things done.[139]

The other relevant provision is section 127 of the Communications Act 2003. This makes it criminal to send by means of a public electronic communications network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character, or causes such messages to be sent.[140] However, it is worth noting that this offence is currently under review by the Law Commission as part of their review into abusive and offensive online communications.[141]

These offences must be viewed as fallbacks. While the majority of online sexual extortion cases may involve conduct that these offences seek to criminalise, this cannot be said to be the primary wrong in these cases. Threats are just one aspect of what is wrong and imposing liability in respect of these offences fails to convey potential additional wrongs such as an unlawful demand, sexual threat, or broader coercive conduct. These offences are therefore relevant but ultimately do not engage with the more serious fundamental wrongs present in online sexual extortion cases.

[137] Criminal Justice and Licensing (Scotland) Act 2010 s.38.
[138] ibid s.38(1).
[139] ibid s.38(3).
[140] Communications Act 2003 s.127.
[141] Law Commission Scoping Report on *Abusive and Offensive Online Communications* (Law Com No 381, 2018) para 4.153.

3.3.2 Non-Consensual Distribution of Intimate Images

The offence of the non-consensual distribution of intimate images[142] was recently introduced to deal with the growing problem of 'revenge porn' and criminalises the disclosure, or threatened disclosure, of an intimate photograph or film. This followed legislation introduced in England and Wales, which had already criminalised the non-consensual disclosure of intimate sexual images.[143] Despite these efforts, this response has been "largely ad hoc"[144] by primarily targeting the vengeful acts of ex-partners.

Both 'revenge porn' and online sexual extortion are part of a group of increasingly prevalent offences comprising IBSA[145] and can involve threats and violations of victims' sexual autonomy, privacy and reputation. However, the problem has been described as one of "square pegs and round holes".[146] The wrongs are fundamentally different. The primary difficulty with this offence is that it only covers one particular type of online sexual extortion: where the threat is the distribution of intimate images or films. As a result, it has been said that "revenge porn laws do not seek to reach this conduct"[147] and that sexual extortion is therefore unlikely to be prosecuted under new legislation.[148]

There are also issues from a labelling perspective. Can the non-consensual distribution of intimate images really be said to capture the wrong in online sexual extortion cases? Even where the distribution of images is part of the conduct, this offence does not capture additional wrongs relating to the creation of sexual extortion material or the coercion of the victim. It is further questionable whether this offence carries a serious enough penalty in cases where there is a greater degree of control, with it carrying a maximum sentence of five years on conviction on indictment.[149]

---

[142] Abusive Harm and Sexual Harm (Scotland) Act 2016 s.2.
[143] Criminal Justice and Courts Act 2015 s.33.
[144] C McGlynn, E Rackley and R Houghton, "Beyond 'revenge porn': the continuum of image-based sexual abuse" (2017) 25 Feminist Legal Studies 25 at 26.
[145] ibid, particularly at 27-29.
[146] B Wittes, C Poplin, Q Jurecic and C Spera, "Closing the sextortion sentencing gap: a legislative proposal" (Center for Technology Innovation at Brookings, 2016) at 7.
[147] ibid.
[148] J Ledward and J Agate, "'Revenge porn' and s.33: the story so far" (2017) 28 Ent. L.R. 40 at 40.
[149] 2016 Act s 2(7)(b).

3.3.3 Stalking

An offence of stalking was introduced[150] in response to growing concerns that stalking was not suitably captured by existing offences (e.g. breach of the peace), both from a labelling perspective and in terms of sentencing.[151] For liability to arise the perpetrator's conduct must cause the victim to suffer fear or alarm,[152] and the conduct must be carried out either with the intention of causing this harm,[153] or where in all the circumstances they ought to have known that this would have that effect.[154] What types of acts might be captured by this offence? A non-exhaustive list is provided in the legislation.[155] Most relevant to online sexual extortion would be contacting, or attempting to contact the victim or other person by any means,[156] publishing any statement or other material relating or purporting to relate to the victim, or purporting to originate from the victim,[157] monitoring the victim's use of the Internet, email or any other form of electronic communication,[158] and watching or spying on the victim or other person.[159] There are parallels between stalking and online sexual extortion. Both may involve a course of conduct and much of the wrong of stalking can be derived from the "intrusion of privacy and personal autonomy".[160] Although not all cases of online sexual extortion constitute a course of conduct, the nature of the wrongdoing makes it difficult to envisage a one-off incident. Indeed, no examples reported in the media or literature have been isolated. Stalking may therefore be relevant insofar as it addresses more long-lasting conduct capable of causing fear, anxiety and emotional distress.

It is worth noting that where such conduct is persistent then this also may constitute harassment. However, under Scots law harassment is part of the civil law[161] and criminal liability does not arise.[162]

---

[150] 2010 Act s.39(1).
[151] Gordon, *Criminal Law* para 48.16.
[152] 2010 Act s.39(2).
[153] ibid s.39(3).
[154] ibid s.39(4).
[155] ibid s.39(6).
[156] ibid s.39(6)(b).
[157] ibid s.39(6)(c).
[158] ibid s.39(6)(d).
[159] ibid s.39(6)(i).
[160] Gordon, *Criminal Law* para 48.16
[161] Protection from Harassment Act 1997 s.8(2).
[162] The exception to this is where there is a breach of a non-harassment order, which is a criminal offence. See ibid s.9(1).

3.3.4 Coercive Control

In some instances, online sexual extortion may be committed by someone personally known to the victim. This conduct may be characterised as a form of coercive control and a means of retaining control over another. This may be to compel them to engage in additional sexual acts or prevent them from seeking judicial intervention or leaving the abuser.[163] Where intimate images are used to carry out extortion, these images are often the result of coercive and abusive behaviour.[164] Legislation has recently been enacted in Scotland to counter this problem by creating a discrete offence of abusive behaviour.[165] This offence applies to spouses or civil partners, and individuals living together as if spouses, or in an intimate personal relationship with one another.[166] This is an obvious limitation of this offence in terms of targeting online sexual extortion. Only in a small proportion of cases will the perpetrator and victim be in such relationship. However, where online sexual extortion does occur in these circumstances it is possible that liability may arise for this offence. For this to happen there must be a course of abusive behaviour[167] which a reasonable person would consider likely to cause the victim to suffer physical or psychological harm.[168] The perpetrator must either intend for this course of behaviour to cause the necessary harm,[169] or be reckless as to this.[170] As with stalking, this offence can be committed in a number of different ways. Firstly, where the behaviour directed at the victim is violent, threatening or intimidating.[171] Secondly, where the purpose of the behaviour is to produce one of the effects listed in the provision,[172] or where a reasonable person would consider the behaviour to bring about one of the effects.[173] Each of these effects could be relevant to online sexual extortion cases. These are: making the victim dependent on, or subordinate to the perpetrator;[174] isolating the victim from friends, relatives or other sources of support;[175] controlling, regulating or monitoring the victim's day-to-day activities;[176] depriving the victim of, or

[163] A Powell and N Henry, *Sexual Violence in a Digital Age* (2017) 123.
[164] D Citron and M Franks, "Criminalizing revenge porn" (2014) 49 Wake Forest L.Rev.345 at 351.
[165] Domestic Abuse (Scotland) Act 2018.
[166] ibid s.11(2).
[167] ibid s.1(1).
[168] ibid s.1(2)(a). Psychological harm is stated as including alarm, fear and distress: s.1(3)
[169] ibid s.1(2)(b)(i).
[170] ibid s.1(2)(b)(ii).
[171] ibid s.2(2)(a).
[172] ibid s.2(2)(b)(i).
[173] ibid s.2(2)(b)(ii).
[174] ibid s.2(3)(a).
[175] ibid s.2(3)(b).
[176] ibid s.2(3)(c).

restricting their freedom of action;[177] and frightening, humiliating, degrading or punishing the victim.[178]

3.4 Evaluation

What does the above discussion tell us about the criminal law response to online sexual extortion? That existing offences may be used to the extent that they impose liability for the individual criminal acts we see in such cases. However, this is quite different from the question of whether they capture the very nature of the wrongdoing. It is argued that they fall short on this ground.

On the first point of availability of offences, it has been shown that a multitude of offences may be used. This provides a number of options for imposing criminal liability. Charging an individual with multiple offences is not on its own problematic.

The relative breadth of offences such as extortion and fraud in contrast to the equivalent English law offences is useful. These offences may be used in a flexible manner, targeting individuals who extort or defraud victims, even where not done for financial gain.

In addition to these common law offences, a number of statutory sexual offences have been identified, particularly those based around sexual coercion and indecent communications. These offences are effective in terms of marking the perpetrator as a sexual offender. This is evidently important in responding to conduct that can cause serious harm to one's sexual autonomy. However, even where an individual is not charged with a 'sexual offence', that the court can subject the offender to the notification requirement procedure in disposing of the case is important.

Recent statutory offences also go some way in encompassing conduct seen in cases of online sexual extortion. Where part of a pattern of broader coercive control in abusive relationships then the new abusive behaviour offence may be used. The offence of non-consensual distribution of intimate images may also be relevant to the extent that it will

[177] ibid s.2(3)(d).
[178] ibid s.2(3)(e).

capture one type of online sexual extortion: where there is a threat to distribute intimate images. However, these offences are only effective in limited circumstances.

This leads us to the second issue: how *suitable* is the current criminal law response to online sexual extortion? In evaluating the criminal law response it is not enough that the law has marked something as wrongful:[179] "what matters is not just that one has been convicted, but of *what* one has been convicted".[180] Although preferable to have offences that impose liability as opposed to none at all, these offences should not simply be accepted as a solution. Why? Because the offences a perpetrator is charged with may not suitably map onto the (i) nature of the wrong, and (ii) harm(s) experienced by the victim. This raises conceptual and practical concerns in terms of our characterisation of the wrong and labelling.

One problem with relying on existing individual offences to prosecute this conduct is that this approach may not adequately capture the nature of the wrongdoing nor the culpability of the offender. Parallels can be drawn here with recent legislation targeting domestic abuse,[181] and modern slavery.[182] In both instances offences already captured the individual criminal acts comprising this conduct. For example, offences of assault and threatening and abusive behaviour would both be relevant in a number of domestic abuse cases. This is similarly the case with modern slavery where there are offences of false imprisonment, extortion, assault and certain sexual offences. However, charging perpetrators of wrongs such as domestic abuse and modern slavery with these individual offences fails to convey the offender's ongoing control and coercion of another individual. That is not to say that charging an individual with different offences such as extortion and causing a person to engage in sexual activity is never appropriate. In some cases it may be, and the combination of these offences would suitably reflect the culpability of the offender and harms experienced by the victims. However, it is particularly in those more serious cases of online sexual extortion, where there is more of an issue.[183]

[179] M Plaxton, "The challenge of the bad man" (2012) 58 McGill LJ 451.
[180] Horder (n.132) at 351.
[181] Domestic Abuse (Scotland) Act 2018. See also Serious Crime Act s.76 for the equivalent offence in England law offence.
[182] Human Trafficking and Exploitation (Scotland) Act 2015 s.4.
[183] Such as those cases that have been characterised as "sexual slavery".

Building on this, it is important that the name given to an offence does more than simply just describe the prohibited conduct, but also "capture[s] the moral essence of the wrong involved".[184] This is referred to as the principle of "fair labelling" and is significant in terms of the accused, victim and wider public.[185] In assessing the effectiveness of substantive criminal law, it is important to ensure that offences suitably label the criminal conduct and map onto the exact nature of the wrong. This is more challenging in this context given that there is no singular offence that responds to the conduct. This means that there is a greater risk that the offence(s) charged may not label the accused's conduct in the most appropriate manner.

Making the perpetrator subject to notification requirements fulfils one key labelling aspect in terms of communicating to the wider public, potential employers and agencies[186] that the individual is a sexual offender. However, this does not solve a broader concern. This is that the label alone does not "accurately describe the nature and magnitude of the wrong in question".[187]

Could we not simply reflect this severity at the sentencing stage? While this would be possible in respect of some of the offences discussed above (e.g. extortion or causing an individual to engage in sexual activity), sentencing has been described as a "very blunt tool for assessing the level of a person's wrongdoing".[188] One reason for this is that it may fail to accurately convey the offender's culpability[189] and this could be because it takes into account other considerations such as discounting or mitigating circumstances.

Furthermore, Chalmers and Leverick identify the symbolic significance of a name as a factor,[190] as is the normative benefit of communicating to criminal justice professionals that such incidents should be taken seriously".[191] They offer a domestic abuse offence as an example of this, with it being important to mark out this conduct as being more culpable than assault.

Online sexual extortion is a clearer label. It communicates exactly what is wrong with the offender's conduct and leaves the wider public in no doubt as to its seriousness. There is no

[184] Horder (n.132) at 335.
[185] G Williams, "Convictions and fair labelling" (1983) 42 CLJ 85 at 85; J Chalmers and F Leverick, "Fair labelling in criminal law" (2008) 71 MLR 217 at 231.
[186] ibid Chalmers & Leverick at 234-235.
[187] Plaxton (n.179) at 470.
[188] Chalmers & Leverick (n.185) at 223.
[189] ibid.
[190] ibid at 241-242.
[191] ibid at 229.

ambiguity concerning the offender's culpability, in contrast with the confusion that may arise where an offender is convicted of a non-sexual offence such as extortion. Even a serious sexual offence such as causing an individual to engage in sexual activity fails to bring out the possible violations to an individual's private life, reputation, and liberty.

Finally, certain offences discussed above are serious as individual wrongs, yet in the context of online sexual extortion may be more accurately characterised as preparatory.[192] What is therefore neglected by charging a person with these offences (e.g. voyeurism; pornography offences) is the accused's wider criminal motivations and arguably heightened culpability. For example, if the accused causes an individual to engage in sexual activity in order to film this activity and use it as a means of later coercing the victim then arguably this shows a greater degree of culpability than where this additional motivation is absent.

In summary, this chapter has explored the different offences that may impose liability in online sexual extortion cases. Beginning with sexual offences, it was found that acts of extortion will likely vitiate consent and that these offences benefit from recognising a victim's sexual harms and in marking the offender as a sexual offender. While other offences were found to be relevant, each had shortcomings, either in terms of their rationales, accurately labelling the accused, the interests they protect, and only applying in limited circumstances. Although the criminal law is collectively able to combat this problem, doubts have been expressed about the manner in which this is done and it is concluded that this approach fails to convey the magnitude of the wrong.

[192] See above at 1.3.4.

4 ADDRESSING THE PROBLEMS

This chapter will build on the previous three chapters by offering solutions to problems identified by this research. These can be separated into two categories: problems with the law and problems that cannot be resolved by legal redress. The chapter will outline these problems and propose how the criminal law can best respond to them. In addressing the latter point, this will draw on conclusions reached in the preceding chapter regarding the effectiveness of the existing criminal law response. It will do so by recommending a legislative solution that will help overcome shortcomings with the current legal framework.

4.1 Legal Barriers

In addressing legal barriers, this chapter will examine issues with the criminal process, with some of the core problems arising *after* the perpetration of the criminal conduct. These include jurisdiction and complainer anonymity.

4.1.1 Jurisdiction

As seen from this research, many perpetrators operate in different jurisdictions from their victims. Although offline sexual offences may span jurisdictions (e.g. sex-trafficking), this is made even more possible with online sexual offending.[1] Any response to online sexual extortion must have regard to its cross-jurisdictional nature and tackle the "anonymity, high-level privacy, invisibility, and the often lack of individual traces that characterize the Internet environment".[2] This is an area where online sexual extortion can be distinguished from similar offline conduct; traditional extortion does not pose "the same inter-jurisdictional and cyber-security problems"[3] as online activities. This was a key issue in the Daniel Perry case in Scotland. The difficulty was not so much identifying the perpetrator, but rather reaching and extraditing them. In addition, there have been reports of online sexual extortion attacks

[1] S Pegg and A Davies, *Sexual Offences: Law and Context* (2016) 175.
[2] A Barak, "Sexual harassment on the Internet" (2005) 23 Social Science Computer Review 77 at 85.
[3] B Wittes, C Poplin, Q Jurecic and C Spera, "Sextortion: cybersecurity, teenagers, and remote sexual assault" (Center for Technology Innovation at Brookings, 2016) at 11.

from other jurisdictions targeting UK citizens. These include the case of a perpetrator acting from the Netherlands who targeted victims in multiple jurisdictions[4] and perpetrators operating from Kuwait.[5] It is acknowledged that there are differences between having criminal offences able to target this conduct, and establishing jurisdiction over individuals operating in other territories.[6] This is a problem applicable to cybercrime more generally and has been considered in detail elsewhere.[7] Thus, for the purposes of this research, despite recognising this barrier, issues relating to online sexual extortion in Scotland will be explored without reference to jurisdiction and extradition.

4.1.2 Complainer Anonymity

Complainer anonymity is another problem with the criminal process that can act as a barrier to justice being achieved. Victims may be reluctant to report abuse they have suffered if they believe that their identity may be disclosed. As the very nature of the offending in online sexual extortion cases concerns intimate details relating to the victim and their sexuality, it would be problematic if such details were to be publicised when reporting this to authorities. It is therefore necessary to ensure that victims can come forward without this risk.

The court has two means of preserving a complainer's anonymity: at common law and under section 11 of the Contempt of Court Act 1981. These were examined by the High Court in *A v Harrower*[8] after the complainer in a summary prosecution for extortion petitioned the *nobile officium*. When called in the Sheriff Court, media reports had published personal details pertaining to the complainer including his name, the nature of threats made against him, and photographs of him. While the sheriff initially made an order providing the complainer with anonymity and prohibiting publication of personal details, this was later recalled. This was because the sheriff did not believe himself to have the power when

[4] H Agerholm, "Dutch man jailed for 10 years for blackmailing victims into webcam sex acts", The Independent, (17 March 2017). Available at: *http://www.independent.co.uk/news/world/europe/webcam-sex-acts-blackmail-dutch-man-jailed-a7635051.html*
[5] P Peachey, "Paedophiles blackmail thousands of UK teens into online sex acts", The Independent, (20 September 2013). Available at: *https://www.independent.co.uk/news/uk/crime/paedophiles-blackmail-thousands-of-uk-teens-into-online-sex-acts-8827794.html*
[6] J Clough, *Principles of Cybercrime* (2015) 475.
[7] ibid Ch 14: "Jurisdiction"; S Brenner, *Cybercrime and the Law: Challenges, Issues and Outcomes* (2012); S Brenner and BJ Koops (eds), *Cybercrime and Jurisdiction: A Global Survey* (2006).
[8] [2017] HCJAC 91.

exercising summary jurisdiction to make an order for anonymity at common law.[9] In finding that that the sheriff did have such a power, the High Court in *Harrower* set out the law in Scotland: that the anonymity of a complainer is within the discretion of the court. This is a common law power that the court holds.[10] The position here can be contrasted with that in England and Wales, where complainers in sexual offence cases have an automatic statutory right to lifelong anonymity.[11]

The court went on to say that they also have power deriving from section 11 of the Contempt of Court Act 1981.[12] This provides that in addition to making a common law anonymity order, "the court may give such directions prohibiting the publication of that name or matter in connection with the proceedings as appear to the court to be necessary for the purpose for which it was so withheld".[13]

In cases of online sexual extortion it is likely on the basis of this decision that extortion victims in Scotland will receive anonymity.[14] This was supported in the Supreme Court by Lord Rodger who in *Re Guardian News and Media Limited*[15] stated *obiter* that the evidence of a victim of blackmail or extortion would be an "obvious example" where the section 11 power might be invoked.[16]

However, while in theory this appears to mitigate concerns that complainers may have in reporting such conduct, two issues remain. Firstly, this protection often comes too late. If the court does not make an order until proceedings begin, or an application is made, then this fails to safeguard the complainer's anonymity at the reporting stage. This is in contrast to England where in respect of sexual offences, anonymity is automatically provided from the reporting stage.

Secondly, press and reputable media outlets will generally be aware of and respect the rules in relation to complainer anonymity. They will likely want to preserve working relationships they have with law enforcement agencies by adhering to these rules. However, the growth of the Internet is problematic and this has similarly been raised as an issue in domestic abuse

[9] ibid at paras 10-11.
[10] ibid at paras 16-21.
[11] Sexual Offences (Amendment) Act 1992 s.1, 2.
[12] *Harrower* at para 27.
[13] Contempt of Court Act 1981 s.11.
[14] *Harrower* at paras 24-25.
[15] [2010] 2 AC 697.
[16] ibid at para 31 per Lord Rodger

cases.[17] An example of this in England is in the Ched Evans rape case, where following his trial nine people were convicted and fined after naming the complainer on Twitter.[18] This problem will continue to arise. Although this example shows that individuals as well as media organisations may be liable for breaching an anonymity order, this may do little to reassure complainers. They may still worry that either their identity or personal details may be posted online, and that despite there being criminal sanctions to punish such individuals, this relies not only on knowing the identity of the person disclosing, but also on being able to prosecute them. Furthermore, as with the disclosure of sexual material in cases of online sexual extortion, once published on the Internet, there is no effective means of preventing its circulation or preventing others from seeing it: the damage is already done.

It is argued that placing complainer anonymity on a statutory footing in Scotland could increase the likelihood of victims of certain crimes reporting these to the police. When might such a rule apply? It would be necessary for it to firstly apply in respect of certain offences. This would allow for automatic anonymity from the moment an offence is reported to the police. This would most obviously apply to sexual offences, but should also extend to offences which may be sensitive in nature or have the potential to violate the privacy or reputation of the complainer (e.g. extortion, and recent statutory offences including coercive control, stalking and the non-consensual distribution of intimate images). It is interesting to note that in England the offence of non-consensual distribution of intimate images does not confer *automatic* anonymity on complainers since it is not regarded as a 'sexual offence'.[19] In encouraging greater levels of reporting and recognising that complainers in other offences would benefit from anonymity, it is suggested that Scots law adopts a broader statutory regime.

However, it is not as straightforward as simply listing offences where anonymity should be conferred. In some cases the wider factual context ought to be taken into account, even where the reported offence would not typically attract anonymity. Such an approach would be consistent with current practice that an order should be made where "regardless of the outcome of the case, the disclosure of that party's identity would constitute an injustice to him; for example, where disclosure would endanger his safety, or would be commercially

[17] M Hughes, "The News Media", in H Hughes (ed), *Domestic Abuse and Scots Law* (2011) 205 at para 10-35.
[18] F Perraudin, "Ched Evans: 10 men cautioned for revealing identity of accuser", The Guardian, (26 Apr 2017). Available at: *https://www.theguardian.com/uk-news/2017/apr/26/ched-evans-10-men-cautioned-for-revealing-identity-of-accuser*. This was a breach of the complainer's right to lifelong anonymity.
[19] J Ledward and J Agate, "'Revenge porn' and s.33: the story of so far" (2017) 28 Entertainment Law Review 40 at 41.

ruinous".[20] An example can be seen in *HM Advocate v M*[21] where the accused was charged with culpably and recklessly infecting the complainer with HIV and Hepatitis C. Due to the sensitive facts in this case, the court made an order preventing disclosure or publication of the name, age, address, nature of employment, ethnic origin or nationality of the complainer.[22] Provision would therefore be needed to ensure that anonymity is not limited only to those offences listed in the statute, but could also apply where the wider factual context makes it appropriate in protecting the complainer. While there would be no practical means of providing for automatic anonymity in these cases, greater certainty could be provided to complainers by placing on a statutory footing those circumstances in which anonymity may be provided. This would allow for complainers to have a better understanding of the circumstances in which they will be able to remain anonymous through the judicial process.

4.2 Non-Legal Barriers

Although this thesis has primarily approached this growing problem from a doctrinal perspective, it is acknowledged that legal remedies can only achieve so much.[23] It will be argued that non-legal barriers represent significant obstacles for victims in obtaining justice. Unless these are overcome in coordination with legal reform, difficulties will remain. This section will consider issues concerning media coverage and under-reporting.

4.2.1 Media Coverage

Although raising awareness is vital, media coverage remains a problem. It has the potential to downplay the severity of online sexual extortion or misrepresent it. This is important in a criminal law context: the media has "significant power in shaping policy".[24] There are two strands to this: the first is to focus on the actions of the victim, while the second is to provide

[20] *A v Secretary of State for the Home Department* [2013] CSIH 43 at para 38 per Lord President Gill.
[21] 2007 SLT 462.
[22] ibid at para 1 per Lord Hodge.
[23] A Powell and N Henry, "Sexual violence in the digital age: the scope and limits of criminal law" (2016) 25 Social and Legal Studies 397 at 411.
[24] Pegg & Davies, *Sexual Offences* (n.1) 14.

narrow or inaccurate coverage of the activity. This section will reach the conclusion that such reporting contributes towards a narrow perception of it.

On this first point, a recurring problem with TFSV is the media's tendency to blame victims for their actions where they have sent intimate images or performed sexual acts online.[25] This is a common reaction to stories of online sexual abuse.[26] In the context of victims of IBSA, this has led to an attribution of responsibility for intimate images being circulated without their consent.[27] This is easily done in online sexual extortion cases too.[28] As set out in the previous chapter, the conduct may be similar. However, both the law and organisations must make clear that where this happens the wrong is not the sending of an image, nor engaging in sexual activity. Rather, it is the presence of a demand backed by a threat. While raising awareness of the problem and warning individuals of online dangers is commendable, this must convey a message that the conduct is wrong. One criticism of the reporting of online sexual extortion cases is that the underlying message detected from articles is that victims should be more careful, suggesting recklessness on their part as contributing to their own victimisation.[29] This requires increased awareness in order to change entrenched attitudes regarding this activity. This in turn will prevent restriction of an individual's positive sexual autonomy, whereby they may be wary of sexually expressing themselves for fear of falling victim to sexual extortion.

Additionally, the types of acts typically reported in the media possess certain characteristics. This reflects a broader issue that media coverage of crime is often inaccurate and "highly selective giving a false picture of criminality".[30] In this context these are often cases that, firstly, have child victims; and secondly, involve deception. This is symptomatic

[25] N Bluett-Boyd, B Fileborn, A Quadara and S Moore, "The role of emerging communication technologies in experiences of sexual violence: a new legal frontier?" (Australian Institute of Family Studies Research Report No.23, 2013) at 34. Available at: *https://aifs.gov.au/publications/role-emerging-communication-technologies-experiences-sexual-violenc*
[26] D Citron, *Hate Crimes in Cyberspace* (2014) 77; A Powell and N Henry, *Sexual Violence in a Digital Age* (2017) 306.
[27] Citron ibid 77.
[28] Wittes et al (n.3) at 23.
[29] Europol European Cybercrime Centre, *Online sexual coercion and extortion as a form of crime affecting children - Law Enforcement Perspective* (May 2017) at 21. Available at: *https://www.europol.europa.eu/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf*
[30] Pegg & Davies, *Sexual Offences* (n.1) 19.

of a wider problem with media coverage of sexual violence[31] that "a considerable portion…of Internet dangers emphasizes young children as potential victims or focuses on violence, abduction, and deception".[32]

Similarly, many reports of online sexual extortion cover those cases where the threat comes from overseas or an organised crime group, which may be less common in reality, but more prominently reported. This is likewise the case with advice provided by the NCA, which focuses on overseas threats while failing to mention activity originating in the UK.[33]

There are also concerns that media reports may be inaccurate, fail to use appropriate legal terminology, and sensationalise particular criminal activity.[34] This has been observed with IBSA where "euphemistic, titillating or narrow language that produces a paradigmatic conceptualization of the behaviour "[35] has been criticised. These problems reinforce the idea that the media may misrepresent conduct and exclude coverage of alternative forms it may take. Disproportionate reporting may, for example, reinforce beliefs that the conduct is only a real threat to children or from overseas crime groups. At a broader level, in terms of emerging sexual offences, education and tackling existing misconceptions and entrenched attitudes among the wider public is necessary.[36] This change must be brought about by organisations and bodies working both within the legal sphere and beyond. Only by doing this can people begin to truly understand the varied nature of the wrongful acts and the potential harmful impact that this conduct may have on different groups.

4.2.2 Victim Reporting

Under-reporting has already been flagged a concern in this thesis.[37] Overcoming this barrier is key. Ensuring that the law is suitably equipped to respond to the conduct is of little practical use if victims are unable to come forward and report instances of wrongdoing. In

[31] T Serisier, "Sex crimes and the media" (2017) Oxford Research Encyclopaedia, Criminology And Criminal Justice. Online publication, available at: *http://oxfordre.com/criminology/view/10.1093/acrefore/9780190264079.001.0001/acrefore-9780190264079-e-118*
[32] J Wolak, D Finkelhor, K Mitchell and M Ybarra, "Online 'predators' and their victims: myths, realities, and implications for prevention and treatment" (2008) 63 American Psychologist 111 at 121-122
[33] NCA information page on "Sextortion". Available at: *https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/kidnap-and-extortion/sextortion-webcam-blackmail*
[34] J Chalmers and F Leverick, "Fair labelling in criminal law" (2008) 71 MLR 217 at 228
[35] Powell & Henry (n.23) at 398.
[36] Horder, *Ashworth's Principles of Criminal Law*, 9th edn (2019) 377.
[37] See above at 2.2.2.

terms of cybercrimes more generally, factors such as embarrassment, lack of knowledge as to what to do, or simply shutting the situation out have been cited as relevant in explaining why victims may not report crimes.[38] It is suggested that reform of complainer anonymity rules, as well as changes to the ways that the media reports cases, would both have the benefit of encouraging greater levels of reporting.

4.3 Proposing a Solution

The final section of this work will draw on conclusions reached above and argue that a legislative response could be the answer. There are two issues to be addressed here: (i) what would the purpose and benefits of this be, and (ii) what would the content consist of?

4.3.1 Purpose and Benefits

As concluded in the previous chapter, a gap exists at present. While current laws criminalise certain conduct present in online sexual extortion cases, they do not do so in the most appropriate manner. The introduction of a distinct offence would help overcome criticisms of the current law. The reasons for this will now be outlined below.

Firstly, although shown that a number of offences may be used in response to this conduct, parallels can be drawn with the introduction of the offence of non-consensual distribution of intimate images in both England and Wales, and Scotland.[39] Existing offences already provided some means of support for victims,[40] but failed to go to the root of the wrongdoing or treat this conduct as a sexual offence.[41] In this respect, the introduction of a statutory offence would follow on from recent reform of sexual offences in Scotland and be consistent

[38] D Wall, *Cybercrime: The Transformation of Crime in the Information Age* (2007) 20.
[39] See above at 3.3.2 for a discussion of this offence.
[40] E.g. Communications Act 2003 s.127.
[41] Scottish Government, Crime and Justice, *Recorded Crime in Scotland, 2017-18* (Sep 2018) at 36. Available at: *https://www.gov.scot/binaries/content/documents/govscot/publications/statistics/2018/09/recorded-crime-scotland-2017-18/documents/recorded-crime-scotland-2017-18/recorded-crime-scotland-2017-18/govscot%3Adocument/recorded-crime-scotland-2017-18.pdf?forceDownload=true*

with the developing pattern of such offences becoming increasingly specific and detailed in nature.[42]

This would combat another problem. It has been argued that legislation targeting the non-consensual distribution of intimate images should cover not only the sharing of these images, but also the creation.[43] This offence would solve this by specifically targeting the non-consensual *creation* of sexual material.

Secondly, it would clearly mark this conduct as a sexual offence. The practical significance of this has been addressed earlier in arguing for this categorisation. It is acknowledged that a key aspect of this - that an offender may still be made subject to the notification requirement procedure - can be met even where they are convicted of a non-sexual offence (e.g. extortion). However, the additional benefit of a distinct sexual offence to capture sexual extortion is that it would give the complainer the same level of protection as those in sexual offence cases. Protections include a prohibition on cross-examining the complainer, a restriction on submitting evidence related to previous sexual history, and being deemed a vulnerable witness. While these results may be achieved in respect of non-sexual offences, having a specific offence allows this to be done automatically without need for application, thereby providing complainers with greater certainty.

Thirdly, there are important consequences from a labelling perspective. One criticism with prosecuting online sexual extortion with existing offences is that it violates the principle of fair labelling. The reasons for this have been stated, but to summarise it would accomplish the following aims: to communicate the severity of the conduct, to make a symbolic statement about the wrong, to raise awareness of the activity, and to more accurately reflect the offender's culpability to those individuals operating both within and outwith the justice system.

Fourthly, legislative intervention would help raise awareness and therefore act as a means of eliminating one of the non-legal barriers outlined earlier. Having a specific offence with a clear label that describes the wrong of the conduct would combat issues relating to media

[42] L Farmer, *Making the Modern Criminal Law* (2016) 287.
[43] C McGlynn and E Rackley, "Image-based sexual abuse" (2017) 37 OJLS 534 at 556.

coverage and be of educational benefit. It would also assist public bodies who would be able to better track the conduct including how often it is reported, prosecuted, and the number of convictions.[44] Increasing awareness can be vital and can be seen through the introduction of the offence of the non-consensual distribution of intimate images. Prior to this offence being introduced in Scotland there had only been five reported convictions for this conduct,[45] yet 421 instances were reported in the period 2017-18 following its enactment in July 2017.[46]

Finally, legislation would provide benefits in terms of sentencing. This thesis will not suggest how perpetrators should be sentenced. However, introducing a specific offence would mitigate two related concerns.

Firstly, it would help ensure that the disposal corresponds to the severity of the wrongdoing. Although certain offences such as sexual coercion or extortion may carry severe sentences, this is not the case with all of the offences discussed above. In particular, while it may be tempting for prosecutors to charge some online sexual extortion conduct with the new non-consensual distribution of intimate images offence, this offence is not intended to confer such severe sentences as are perhaps merited by the conduct seen in the cases discussed.

The second problem relates to an issue raised in the third chapter. This is that having a number of offences that can be used in response to online sexual extortion cases may lead to greater disparity in the sentencing of offenders. This could to some extent be remedied by an individual offence and would also help enhance predictability in respect of the consequences of engaging in the proscribed conduct.

Before considering the content of a new offence, opportunity will be taken to consider two criticisms that may be levelled at this proposal. One is from an over-criminalisation perspective: is the creation of an additional offence really desirable, particularly when existing offences already provides a means of redress? A new offence would not be an example of over-criminalisation in the traditional sense. Rather it would be an example of "more intensive criminalisation of areas that are already covered by the criminal law, as new

[44] B Wittes, C Poplin, Q Jurecic and C Spera, "Closing the sextortion sentencing gap: a legislative proposal" (Center for Technology Innovation at Brookings, 2016) at 7.
[45] D Leask, "Calls for legislation to tackle the spread of 'revenge porn'", The Herald, (11 April 2014). Available at: http://www.heraldscotland.com/news/13155032.Callforlegislationtotacklethespreadofrevengeporn/
[46] Scottish Government, *Recorded Crime* (n.41) at 2.

offences are created to recognise more specific forms of wrongdoing".[47] However, such an approach is criticised by Husak who argues that "overlapping crimes" are problematic.[48] The main concern raised is that this can lead to "charge stacking" and unduly severe sentences for offenders who may be charged with multiple offences.[49] Interestingly, it is suggested that a new offence may have the opposite effect in this jurisdiction by providing a singular offence with which a perpetrator may be charged with, as opposed to multiple offences (including a mixture of sexual offences, dishonesty offences and offense against the person) as seen at present. It is also contended that the argument in favour of a legislative solution has been made out by reference to fair labelling, categorisation, sentencing, increased awareness, and more accurately capturing the essence of the wrong; factors which Husak fails to mention as being relevant in questioning the need for "overlapping offences".[50]

The second concerns responding to conduct in an *ad hoc* manner.[51] It is acknowledged that there is the need for a comprehensive and over-arching review of the law relating to sexual cybercrime - which would encompass much of IBSA - but also reach beyond this to include TFSV. However, the law faces a difficult task in this area. While a review would allow for a more principled consideration of this offending, this would take some time and the law cannot allow itself to fall further behind when it comes to cybercrime. Furthermore, the proposals set out in this thesis and undertaking a review are not mutually exclusive. It is hoped that this thesis could assist with future research and encourage a broader review of this field.

4.3.2 Content

What would a legislative answer look like? This final section will resolve this question by drawing on the benefits set out above and the problems identified with the existing law.

Firstly, it is important that a statutory offence does not make any distinction based on the age or gender of the relevant parties, nor the relationship between them. As shown, one limitation of existing offences is that some target specific types of conduct. For example,

[47] Farmer, *Modern Criminal Law* (n.42) 105.
[48] D Husak, *Overcriminalization: The Limitations of the Criminal Law* (2008) 37
[49] ibid 38.
[50] ibid 37ff.
[51] McGlynn & Rackley (n.43) at 551.

coercive control only applies to individuals in an intimate relationship together, while grooming is aimed at protecting children. This is not a criticism of these offences. They have clear aims in terms of the conduct they criminalise and much of the rationale of these offences is to raise awareness that these acts are criminal, to more effectively label the criminal wrongs, and to make a symbolic statement about the culpability of perpetrators. However, as established in the first chapter, online sexual extortion is not confined to one particular group of people, nor any specific context.

Secondly, legislation should clearly reflect online sexual extortion's status as a sexual offence. This is consistent with the conclusion reached in Chapter 2 that this conduct must necessarily involve some violation of an individual's sexual autonomy, either through a threat to do something, or a demand having a similar effect. By unambiguously categorising the offence in this way, it avoids problems English law has encountered with its offence of non-consensual distribution of intimate images not being classified as a sexual offence.[52] From a Scottish perspective, this would mitigate concerns over 'non-sexual offences' (e.g. extortion) being used to target what is primarily a sexual wrong.

Thirdly, ensuring sufficient breadth is key. While this thesis has focused solely on the issue of *online* sexual extortion for the reasons set out in Chapter 2, any legislative answer must be framed in broader terms. Although technology has allowed this conduct to be perpetrated in multiple ways and in a more pervasive manner, it is still possible that this conduct may either be carried out offline (or at least partly offline). In particular, conduct may begin online but later continue offline. It is the course of conduct that must be captured. In proposing legislation there would be no reason to exclude offline conduct other than that it may occur less frequently and be more difficult to carry out without using technology to some extent.[53] These are not sound reasons for doing this and the offence, although targeted at conduct which primarily manifests itself online, should not be restricted to this.

[52] Ledward & Agate (n.19) at 41.
[53] In a study into victims of both online and offline sexual extortion it was found that even in those cases that originated offline, 98% of respondents reported being coerced through technology by the perpetrator:
J Wolak and D Finkelhor, "Sextortion: findings from a survey of 1,631 victims" (Crimes Against Children Research Center, 2016) at 11. Available at: *https://www.wearethorn.org/wp-content/uploads/2016/08/Sextortion_Report.pdf*

Fourthly, what would the proscribed conduct be? Sexual extortion is the real issue. While individual offences criminalise specific wrongs such as voyeurism, grooming, and the non-consensual distribution of intimate images, this research has exposed the lack of any offence that really gets to grips with *prolonged* sexual extortion. A statutory offence could remedy this by criminalising the pattern of conduct, as opposed to simply individual acts. This would recognise the ways that the Internet and technology may cause continuing harm. The offence of causing an individual to engage in sexual activity fails to capture prolonged spells of control. The wrongful act in cases of online sexual extortion is not just that of causing a person to engage in sexual activity. As a result, liability should not arise simply at the moment an individual engages in such activity against their will. It is for this reason that the Home Office stated that the rationale for a separate offence of coercive control was to set out "the importance of recognising the harm caused by coercion or control, the cumulative impact on the victim and that a repeated pattern of abuse can be more injurious and harmful than a single incident of violence".[54] Given the earlier examination of the nature of the harms, this is equally appropriate in this context.

How might such an offence be drafted? The content of a new offence could draw inspiration from recently introduced legislation aimed at criminalising coercive control. Coercive control was defined by the Home Office as "[c]ontrolling or coercive behaviour [that] does not relate to a single incident, it is a purposeful pattern of behaviour which takes place over time in order for one individual to exert power, control or coercion over another".[55] These are the type of acts in the context of online sexual extortion that it has been argued for the reasons above are not adequately captured by existing laws.

It is proposed that the *actus reus* retains similarities with the common law offence of extortion. The wrongful act is the perpetrator's demand backed by a threat. What distinguishes this from extortion is the specific requirement of a sexual element. As proposed in the first chapter, online sexual extortion should be characterised by the presence of a threat and demand, at least one of which is sexual in nature. In ensuring consistency with existing legislation on sexual offences, 'sexual' for the purposes of this offence should be defined as

[54] Home Office, *Controlling or Coercive Behaviour in an Intimate or Family Relationship: Statutory Guidance Framework* (Dec 2015) 3.
[55] ibid.

it is in the 2009 Act. This by reference to its ordinary meaning: whether or not a reasonable person would, in all the circumstances of the case, consider the act sexual.[56]

The *actus reus* of the offence would be satisfied where either (i) A makes a demand from B, and this demand is backed by a sexual threat, or (ii) where A makes a sexual demand from B, and this sexual demand is backed by a threat.

This would be a differentiated offence that could be committed in a number of ways, thereby reflecting the various types of conduct present in online sexual extortion cases. For this reason, the terms "threats" and "demands" should be broadly construed[57] in order to give the provisions a degree of flexibility in capturing the various types of threats and demands. In order to supplement the wording in the offence, a non-exhaustive list of the types of acts falling within the scope of "sexual demand" and "sexual threat" would be beneficial.

A suggestion as to how this could be set out is provided below:

"Sexual demand" would include, among others, demands by A that B:

- provides a sexual image or video-recording
- engages in a sexual act
- accesses or views pornography

"Sexual threat" would include, among others, threats by A to:

- send, publish, or distribute a sexual image or video-recording of B
- commit a sexual offence against B
- release other sexual material relating to B

The following observations are expected to assist with how this offence may appear in legislation:

- In recognising different modes of communications, demands and threats may be communicated in writing or verbally.

[56] 2009 Act s.60(2)
[57] See 3.2.1; *Silverstein v HM Advocate* 1949 JC 160

- "Sexual image" would be an image "produced by whatever means and whether or not a moving image" as defined for the purposes of the offence of coercing a person into looking at a sexual image.[58]
- "Sexual act" would include acts engaged in whether by B alone, by B with A, or by B with a third party. This would also include exposure of B's genitals or buttocks.
- Including the term "sexual material" ensures that a threat to distribute material that may not be an image or video is included within the scope of "sexual threat". This might include personal information relating to B's sexuality such as sexual orientation and sexual preferences, or images or recordings of sexual communications from B.
- Reference is made to "psychological harm"[59] as it encompasses a wider range of mental harms than fear, alarm and distress. This would ensure that harms are recognised in respect of invasions of privacy or damage to reputation, both of which may cause B psychological harm (e.g. anxiety). However, physical harm should also be included in order to capture situations where the victim is coerced into physically harming themselves.

In terms of the *mens rea*, the starting point should be that the perpetrator intends the conduct (i.e. the demand backed by a threat). Thus, A must intentionally communicate to B a demand backed by a threat in accordance with the conduct element stated above. This means that only cases where A specifically targets and directs threats and demands at B will be caught by the offence. Drawing on the recently introduced abusive behaviour offence, a requirement that A either does this with the intention to cause physical or psychological harm to B, or is reckless as to whether B suffers such harm, is recommended. This will allow for a wide range of motives to be included, and does not limit the criminal activity to only cases where A intends to cause harm to B. As has been shown, in some cases this intention is absent and A acts for an altogether different motive. This does not reduce B's harm and this is why recklessness as to the harm should suffice.

It is hoped that an offence based on these recommendations may help address the issue of online sexual extortion in Scotland. As well as providing a singular offence for convicting

[58] 2009 Act s.6(3)
[59] Domestic Abuse (Scotland) Act 2018 s.1(3)

individuals that suitably reflects the scale of the wrongdoing, the harms suffered by victims, and appropriately labels the conduct, this would have the additional benefit of raising awareness of the behaviour and sending a message as to its seriousness.

CONCLUSION

This thesis has sought to examine online sexual extortion as an emerging species of conduct and identify how the criminal law can best respond to this issue in Scotland. In achieving this, the research has proposed a definition of online sexual extortion, identified and assessed the harms, undertaken an evaluation of the current criminal law response, and suggested possible improvements to the legal response.

The first chapter aimed to define online sexual extortion. Drawing on existing definitions and terminology used in the literature, a broad definition of online sexual extortion was proposed. This reflects the different ways that the conduct may violate an individual's sexual autonomy and ensures that this is the defining element of the wrong. In order to give this definition substance, a typology of the different modes of perpetration was set out, with the benefit of providing illustrative examples of the many ways in which the wrong may be perpetrated.

The second chapter was broader in scope. The first aim was to map online sexual extortion in Scotland. This was done by reviewing existing literature, and then through an analysis of statistical data. While some statistical evidence and media coverage pointed towards this being a growing threat in Scotland, academic literature and public reports have paid little attention to it. Factors such as under-reporting, problems with recording practices, and the lack of a distinct offence were found to make it difficult to assess recorded cases. This fuels the need for a detailed consideration of the issue in Scotland.

Focus then turned to the harms of online sexual extortion. The second aim of the chapter was to identify the interests threatened by this conduct. The development of sexual extortion as a distinct wrong was shown, and it was submitted that technological developments altered the nature of this wrong and the harms felt. It was argued that breach of sexual autonomy represents the primary harm, and that online sexual extortion must be characterised as a sexual offence for both conceptual and practical reasons. However, it additionally has the potential to violate financial, privacy and reputational interests, particularly given the threat it poses from overseas organised crime groups and to individuals' virtual identities.

The overarching aim of the third chapter was to evaluate the criminal law response to online sexual extortion in Scotland. It was firstly shown that the conduct straddles different offence groups and cannot be neatly placed in one category, this being consistent with the findings in the second chapter. Various offences were found to deal with features prevalent in online sexual extortion cases. In evaluating these offences, the conclusion reached is that the problem is not so much a gap in the law, but rather a strained application of the law. The legal tools are there; however, existing offences do not address the conduct in the most appropriate manner. This is because they fail to: (i) accurately label the conduct, (ii) convey the seriousness of it, (iii) capture the nature of the wrongs, and (iv) reflect the harms experienced by victims.

The purpose of the fourth chapter was firstly to look beyond substantive criminal law. It was argued that legal reform can only achieve so much. Other barriers to progress being made had to be considered. These fell into two categories: barriers relating to the criminal process and non-legal barriers. While only reform of the first category can be achieved through legal redress, the two categories are inter-related. Under-reporting could be mitigated if complainer anonymity was guaranteed through suggested reform of these rules. Similarly, while media reporting may perpetuate lack of awareness or understanding of the issues, these concerns could be overcome by legislative intervention.

In terms of providing a solution to the problem of online sexual extortion, reform of the law was proposed. It was argued that there is scope for a discrete offence dealing with sexual extortion. The principles to which this should conform to were set out and it was suggested that a new offence would not be vulnerable to the same criticisms as the existing criminal law framework. It would more accurately label the conduct, clearly mark it as a sexual offence, reflect the harms suffered by victims, and provide benefits in terms of sentencing and raising awareness. It is hoped that thought may therefore be given to the proposals outlined in this thesis and that improvements can be made to the law's response to this species of wrongdoing, as well as other types of IBSA and TFSV.

BIBLIOGRAPHY

Books

A Alison, *Principles of the Criminal Law of Scotland* (1832)

A Ashworth and J Horder, *Principles of Criminal Law*, 7th edn (2013)

S Bremner, *Cybercrime: Criminal Threats from Cyberspace* (2010)

S Brenner, *Cybercrime and the Law: Challenges, Issues and Outcomes* (2012)

S Brenner and BJ Koops (eds), *Cybercrime and Jurisdiction: A Global Survey* (2006)

D K Citron, *Hate Crimes in Cyberspace* (2014)

J Clough, *Principles of Cybercrime*, 2nd edn (2015)

M Cross, *Social Media Security* (2014)

A M Cubie, *Scots Criminal Law*, 4th edn (2016)

A Cudd and M Navin (eds), *Core Concepts and Contemporary Issues in Privacy* (2018)

L Farmer, *Making the Modern Criminal Law* (2016)

P Ferguson and C McDiarmid, *Scots Criminal Law: A Critical Analysis*, 2nd edn (2014)

A Gillespie, *Cybercrime: Key Issues and Debates* (2015)

G H Gordon, *Criminal Law of Scotland*: Vol 2, 4th edn, by J Chalmers and F Leverick (2016)

P Grabosky, *Cybercrime* (2016)

M Hepworth, *Blackmail* (1975)

J Herring, *Criminal Law: Text, Cases, and Materials*, 3rd edn (2008)

J Horder, *Ashworth's Principles of Criminal Law*, 9th edn (2019)

D Hume, *Commentaries on the Law of Scotland, Respecting Crimes* (1797)

D Husak, *Overcriminalization: the limitations of the criminal law* (2008)

Y Jewkes (ed), *Crime Online* (2007)

Y Jewkes and M Yar (eds), *Handbook of Internet Crime* (2013)

T Jones and I Taggart, *Criminal Law*, 7th edn (2018)

A McLaren, *Sexual Blackmail: A Modern History* (2002)

D Ormerod and K Laird, *Smith and Hogan's Criminal Law*, 14th ed (2015)

D Ormerod and D Williams, *Smith's Law on Theft*, 9th ed (2007)

S Pegg and A Davies, *Sexual Offences: Law and Context* (2016)

A Powell and N Henry, *Sexual Violence in a Digital Age* (2017)

P H Robinson, *Criminal Law* (1997)

P Rook and R Ward, *Rook & Ward on Sexual Offences: Law and Practice*, 5th edn (2016)
A P Simester, J R Spencer, F Stark, G R Sullivan and G J Virgo, *Simester and Sullivan's Criminal Law: Theory and Doctrine*, 6th edn (2016)
T Thomas, *Reporting and Recording Sexual Offences* (2016)
D Wall (ed), *Crime and the Internet* (2001)
D Wall, *Cybercrime: The Transformation of Crime in the Information Age* (2007)
D Wall (ed), *Crime and Deviance in Cyberspace* (2009)
M Wasik, *Crime and the Computer* (1991)

Chapters in Edited Works

J Blackie and J Chalmers, "Mixing and matching in Scottish delict and crime", in M Dyson (ed), *Comparing Tort and Crime* (2015) 271
L Campbell and S Cowan, "The relevance of sexual history and vulnerability in the prosecution of sexual offences", in P Duff and P Ferguson (eds), *Scottish Criminal Evidence Law: Current Developments and Future Trends* (2018) 67
S Green, "What are the sexual offences?", in C Flanders and Z Hoskins (eds), *The New Philosophy of Criminal Law* (2016) 57
M Hughes, "The News Media", in H Hughes (ed), *Domestic Abuse and Scots Law* (2011) 205
Y Jewkes and M Yar, "Introduction: the Internet, cybercrime and challenges of the twenty-first century", in Y Jewkes and M Yar (eds), *Handbook of Internet Crime* (2013) 1
S Lee, "The nature and value of privacy", in A Cudd and M Navin (eds), *Core Concepts and Contemporary Issues in Privacy* (2018) 47
R O'Connell, "From fixed to mobile Internet: the morphing of criminal activity online", in M Calder (ed), *Child Sex Abuse and the Internet: Tackling the New Frontier* (2004) 37
W L Robinson, "Digitizing privacy", in A E Cudd and M C Navin (eds), *Core Concepts and Contemporary Issues in Privacy* (2018) 189
C N Stoddart, "Extortion, corruption and related offences", in *The Laws of Scotland: Stair Memorial Encyclopaedia*, Reissue (2005)
M Todd, "Virtual violence: cyberspace, misogyny and online abuse", in T Owen, W Noble and F Speed (eds), *New Perspectives on Cybercrime* (2017) 141
D Wall, "Criminalising cyberspace: the rise of the Internet as a crime problem", in Y Jewkes and M Yar (eds), *Handbook of Internet Crime* (2013) 88

A Wertheimer, “Consent to sexual relations”, in A Wertheimer and F Miller (eds), *The Ethics of Consent: Theory and Practice* (2009) 195

Journal Articles

P Alldridge, “Attempted murder of the soul: blackmail, privacy and secrets” (1983) 13 OJLS 368
A Barak, “Sexual harassment on the Internet” (2005) 23 Social Science Computer Review 77
A Ben-Ze’ev, “Privacy, emotional closeness, and openness in cyberspace” (2003) 19 Computers in Human Behavior 457
J Chalmers and F Leverick, “Fair labelling in criminal law” (2008) 71 MLR 217
D Citron and M Franks, “Criminalizing revenge porn” (2014) 49 Wake Forest L.Rev.345
J Ledward and J Agate, “’Revenge porn’ and s.33: the story of so far” (2017) 28 Entertainment Law Review 40
P Grabosky, “Virtual criminality: old wine in new bottles” (2001) 10 Social and Legal Studies 243
M D Griffiths, “Internet corporate blackmail: a growing problem” (2004) 168 Justice of the Peace 632
J Horder, “Rethinking non-fatal offences against the person” (1994) 14 OJLS 335
C McGlynn and E Rackley, “Image-based sexual abuse” (2017) 37 OJLS 534
C McGlynn, E Rackley and R Houghton, “Beyond ‘revenge porn’: the continuum of image-based sexual abuse” (2017) 25 Feminist Legal Studies 25
C McGlynn and E Rackley, “Image-based sexual abuse: more than just ‘revenge porn’” (2016) Research Spotlight Publication
M G McGrath and E Case, “Forensic psychiatry and the Internet” (2002) J Am Acad Psychiatry Law 81
R Patton, “Taking the sting out of revenge porn: using criminal statutes to safeguard sexual autonomy in the digital age” (2015) 16 Georgetown Journal of Gender and the Law 407
A Powell and N Henry, “Sexual violence in the digital age: the scope and limits of criminal law” (2016) 25 Social and Legal Studies 397
E Quayle, “Over the Internet, under the radar: online child sex abuse and exploitation – a brief literature review” (2017)
M Plaxton, “The challenge of the bad man” (2012) 58 McGill LJ 451

A Powell and N Henry, “Embodied harms: gender, shame, and technology-facilitated sexual violence” (2015) 21 Violence Against Women 758
T Serisier, “Sex crimes and the media” (2017) Oxford Research Encyclopaedia, Criminology and Criminal Justice. Online publication, available at: *http://oxfordre.com/criminology/view/10.1093/acrefore/9780190264079.001.0001/acrefore-9780190264079-e-118*
J Suler, “Online disinhibition effect” (2004) 7 Cyber Psychology & Behavior 321
G Syrota, “Rape: when does fraud vitiate consent?” (1995) 25 Western Australian Law Review 334
K Veli “Sexual extortion of children in cyberspace” (2016) 10 International Journal of Cyber Criminology 110
G Williams, “Convictions and fair labelling” (1983) 42 CLJ 85
B Wittes, “Cyber sextortion and international justice” (2017) 48 Georgetown Journal of International Law 941
B Wittes, C Poplin, Q Jurecic and C Spera, “Closing the sextortion sentencing gap: a legislative proposal” (Center for Technology Innovation at Brookings, 2016)
B Wittes, C Poplin, Q Jurecic and C Spera, “Sextortion: cybersecurity, teenagers, and remote sexual assault” (Center for Technology Innovation at Brookings, 2016)
J Wolak, D Finkelhor, K Mitchell and M Ybarra, “Online ‘predators’ and their victims: myths, realities, and implications for prevention and treatment” (2008) 63 *American Psychologist* 111

Reports

N Bluett-Boyd, B Fileborn, A Quadara and S Moore, “The role of emerging communication technologies in experiences of sexual violence: a new legal frontier?” (Australian Institute of Family Studies Research Report No.23, 2013). Available at: *https://aifs.gov.au/publications/role-emerging-communication-technologies-experiences-sexual-violenc*
Europol European Cybercrime Centre, *Online sexual coercion and extortion as a form of crime affecting children - Law Enforcement Perspective* (May 2017). Available at: *https://www.europol.europa.eu/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf*
Europol, *Internet Organised Crime Threat Assessment (IOCTA) Report* (2017). Available at: *https://www.europol.europa.eu/sites/default/files/documents/iocta2017.pdf*

Home Affairs Select Committee: E-crime (2013, 5th Report of the Home Affairs Select Committee) HC 70

Home Office, *Controlling or Coercive Behaviour in an Intimate or Family Relationship: Statutory Guidance Framework* (Dec 2015)

Home Office, *Cyber-crime: a review of the evidence (Research Report 75), Ch 3, Cyber-enabled crimes – sexual offending against children* (Oct 2013).

Home Office, *Explanatory Notes to the Sexual Offences Act 2003* (2003)

International Association of Women Judges (IAWJ), *Stopping the Abuse of Power Through Sexual Exploitation: Naming, Shaming and Ending Sextortion* (2012)

Law Commission Scoping Report on *Abusive and Offensive Online Communications* (Law Com No 381, 2018)

Police Scotland, *Scottish crime recording standard and Scottish government counting rules* (Apr 2019) at 48. Available at: *https://www2.gov.scot/Resource/0054/00547065.pdf*

Report on *Rape and Other Sexual Offences* (Scot Law Com No 209, 2007)

Scottish Government, Crime and Justice, *Cyber-Crime in Scotland: A Review of the Evidence* (Mar 2018). Available at: *http://www.gov.scot/Resource/0053/00532978.pdf*

Scottish Government, Crime and Justice, *Recorded Crime in Scotland, 2017-18* (Sep 2018). Available at: *https://www.gov.scot/binaries/content/documents/govscot/publications/statistics/2018/09/recorded-crime-scotland-2017-18/documents/recorded-crime-scotland-2017-18/recorded-crime-scotland-2017-18/govscot%3Adocument/recorded-crime-scotland-2017-18.pdf?forceDownload=true*

Scottish Government, Crime and Justice, *Recorded Crime in Scotland, 2016-17* (Sep 2017). Available at: *http://www.gov.scot/Resource/0052/00525033.pdf*

Scottish Government, Crime and Justice, *Recorded Crime in Scotland: Other Sexual Crimes, 2013-14 and 2016-17* (Sep 2017). Available at: *http://www.gov.scot/Resource/0052/00525033.pdf*

Subgroup Against the Sexual Exploitation of Children, NGO Group for the Convention on the Rights of the Child, "Semantics or Substance? Towards a shared understanding of terminology referring to the sexual abuse and exploitation of children" (Jan 2005). Report available at: *www.ecpat.org/wp-content/uploads/legacy/Semantics%20or%20Substnce.pdf*

Trend Micro Report, "Sextortion in the Far East" (2015) at 12. Available at: *https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/sextortion-in-the-far-east-blackmail-goes-mobile*

J Wolak and D Finkelhor, “Sextortion: findings from a survey of 1,631 victims” (Crimes Against Children Research Center. 2016). Available at: *https://www.wearethorn.org/wp-content/uploads/2016/08/Sextortion_Report.pdf*

Media Articles and Press Releases

H Agerholm, “Dutch man jailed for 10 years for blackmailing victims into webcam sex acts”, The Independent, (17 Mar 2017). Available at: *http://www.independent.co.uk/news/world/europe/webcam-sex-acts-blackmail-dutch-man-jailed-a7635051.html*

G Brown, “Sextortion scammers targeting Angus residents in ‘nasty’ con”, The Courier (20 Jul 2018) Available at: *https://www.thecourier.co.uk/fp/news/local/angus-mearns/691358/sextortion-scammers-targetting-angus-residents/*

J Brown, “Experts warn of rise in Internet blackmail as police probe suicide of Daniel Perry”, The Independent, (16 Aug 2013). Available at: *http://www.independent.co.uk/news/uk/crime/experts-warn-of-rise-in-internet-blackmail-as-police-probe-suicide-of-daniel-perry-8769748.html*

A Cramb, “Teenage committed suicide ‘after being blackmailed on Skype’”, Daily Telegraph (15 Aug 2013). Available at: *https://www.telegraph.co.uk/news/uknews/crime/10245809/Teenager-commited-suicide-after-being-blackmailed-on-Skype.html*

A Crawford, “British men 'increasingly' targeted by sextortion”, BBC News, (25 May 2018). Available at: *https://www.bbc.co.uk/news/av/uk-44260271/british-men-increasingly-targeted-by-sextortion?intlink from url=https%3A%2F%2Fwww.bbc.co.uk%2Fnews%2Ftopics%2Fcgdz91y340mt%2Fsextortion&link_location=live-reporting-map*

A Day, C Milmo, D Mort et al, “Scotland witnessing “significant” growth in cybercrime”, The Scotsman, (22 Jul 2017). Available at: *https://www.scotsman.com/future-scotland/tech/scotland-witnessing-significant-growth-in-cyber-crime-1-4511044*

Law Commission press release, “Government asks Law Commission to look at trolling laws” (6 Feb 2018) Available at: *https://www.lawcom.gov.uk/government-asks-law-commission-to-look-at-trolling-laws/*

D Leask, “Calls for legislation to tackle the spread of ‘revenge porn’”, The Herald, (11 Apr 2014). Available at:

http://www.heraldscotland.com/news/13155032.Callforlegislationtotacklethespreadofrevengeporn/

D Lee, "Teenager's death sparks cyber-blackmailing probe", BBC News, (16 Aug 2013). Available at: *http://www.bbc.co.uk/news/uk-scotland-edinburgh-east-fife-23712000*

N Massey, "Sextortion: rise in blackmail-related suicides over sexual images shared online", The Independent, (30 Nov 2016). Available at: *http://www.independent.co.uk/news/uk/home-news/sextortion-rise-suicides-blackmailing-sexual-images-sharing-social-media-a7446776.html*

National Crime Agency information page on "Sextortion". Available at: *https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/kidnap-and-extortion/sextortion-webcam-blackmail*

F Perraudin, "Ched Evans: 10 men cautioned for revealing identity of accuser", The Guardian, (26 Apr 2017). Available at: *https://www.theguardian.com/uk-news/2017/apr/26/ched-evans-10-men-cautioned-for-revealing-identity-of-accuser*

Police Scotland news bulletin, "Men more likely to fall victim to sextortion" (14 Dec 2016). Available at: *http://www.scotland.police.uk/whats-happening/news/2016/december/men-more-likely-to-fall-victim-to-sextortion*

Police Scotland news bulletin, "Webcam extortion warning – Lanarkshire" (23 Aug 2016). Available at: *http://www.scotland.police.uk/whats-happening/news/2016/august/webcam-extortion-warning-lanarkshire*

Police Scotland webpage, "Registered Sex Offender Management". Available at: *https://www.scotland.police.uk/about-us/police-scotland/specialistcrime-division/national-offender-management-unit-new/registered-sex-offender-management*

P Peachey, "Paedophiles blackmail thousands of UK teens into online sex acts", The Independent, (20 Sep 2013). Available at: *https://www.independent.co.uk/news/uk/crime/paedophiles-blackmail-thousands-of-uk-teens-into-online-sex-acts-8827794.html*

P Sherlock, "Revenge pornography victims as young as 11, investigation finds", BBC News, (27 Apr 2016). Available at: *https://www.bbc.co.uk/news/uk-england-36054273*

D Whitworth, "Sextortion: big rise in victims 'with tens of thousands at risk'", BBC News (24 May 2018). Available at: *https://www.bbc.co.uk/news/newsbeat-43433015*

L Williams, "Mystery 'young attractive woman' gets men to do sex acts on Skype - then blackmails them", The Independent, (8 Oct 2015). Available at: *http://www.independent.co.uk/news/young-men-blackmailed-after-being-encouraged-to-perform-sex-acts-on-skype-a6686671.html*

"Andrew McBride jailed for online sexual blackmail campaign", BBC News (14 Jan 2015). Available at: *http://www.bbc.co.uk/news/uk-scotland-glasgow-west-30814443*
"Matthew Falder posed as female artist for online sex attacks" BBC News (16 Oct 2017). Available at: *http://www.bbc.co.uk/news/uk-england-birmingham-41640079*

All of the hyperlinks cited in this thesis have been checked and are valid as of the date of submission.

Cases

A v Harrower [2017] HCJAC 91
A v Secretary of State for the Home Department [2013] CSIH 43
Adcock v Archibald 1925 JC 58
Black v Carmichael 1992 SLT 897
HM Advocate v M 2007 SLT 462
Jas Miller (1862) 4 Irv 238
Kidd v McGowan [2012] HCJAC 163
McHugh v Harvie [2015] HCJAC 86
R v Bingham [2013] EWCA Crim 823
R v Breakwell [2009] EWCA Crim 2998
R v Casabolt [2016] EWCA Crim 1377
R v Clarence (1888) 22 QBD 23
R v Devonald [2008] EWCA Crim 527
R v Hadjou (1989) 11 Cr. App. R. (S.) 29
R v Jheeta [2007] EWCA Crim 1699
R v Kewell [2000] 2 Cr. App. R. (S.) 38
R v Knight (Jordan) [2017] EWCA Crim 1940
R v Linekar [1995] 3 All ER 69
R v Mackie 2013 ABPC 116
R v Papadimitropolous (1957) 98 CLR 249
R v Stone (1989) 11 Cr. App. R. (S.) 176
Rae v Donnelly 1982 SCCR 148
Re Guardian News and Media Limited 2010 2 AC 697
Silverstein v HM Advocate 1949 JC 160

Sunderland (Adam) v HM Advocate [2017] HCJAC 22
WD v McPherson 2013 SCCR 305
White v HM Advocate [1999] 4 WLUK 327
Whyte v HM Advocate 2017 JC 262

Sentencing Statements

HM Advocate v Joshua Hunter, sentencing statement published on Judiciary of Scotland website per Lady Scott. Available at: *http://www.scotland-judiciary.org.uk/8/2057/HMA-v-Joshua-Hunter*
HM Advocate v Andrew McBride, sentencing statement published on Judiciary of Scotland website per Lord Turnbull. Available at: *http://www.scotland-judiciary.org.uk/8/1360/HMA-v-ANDREW-MCBRIDE*

United Kingdom Statutes and Statutes of the Scottish Parliament

Abusive Behaviour and Sexual Harm (Scotland) Act 2016
Civic Government (Scotland) Act 1982
Communications Act 2003
Computer Misuse Act 1990
Contempt of Court Act 1981
Criminal Justice and Courts Act 2015
Criminal Justice and Licensing (Scotland) Act 2010
Criminal Procedure (Scotland) Act 1995
Domestic Abuse (Scotland) Act 2018
Fraud Act 2006
Human Rights Act 1998
Human Trafficking and Exploitation (Scotland) Act 2015
Protection from Harassment Act 1997
Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005
Serious Crime Act 2015
Sexual Offences (Amendment) Act 1992
Sexual Offences Act 2003
Sexual Offences (Scotland) Act 2009
Theft Act 1968