Crime Science

RESEARCH

Open Access

Crime script analysis for adult image-based sexual abuse: a study of crime intervention points for retribution-style offenders

Abigail C. O'Hara[1*], Ryan K. L. Ko[2], Lorraine Mazerolle[1*] and Jonah R. Rimer[1]

Abstract

Objective: This research uses crime scripts to understand adult retribution-style image-based sexual abuse (RS-IBSA) offender decision-making and offending in offline and online environments. We explain the crime-commission process of adult RS-IBSA and identify crime intervention points at eight crime script stages.

Methods: Publicly released court transcripts of adult RS-IBSA prosecution cases (n = 18) in New Zealand from 2015 to 2018 were utilised to examine the crime-commission process of adult RS-IBSA. We analysed the court transcripts thematically at offence-level prior to constructing the crime scripts.

Findings: The study identified four types of adult RS-IBSA acts including the non-consensual dissemination of a victim's intimate images, violent cyber sextortion, covert intimate photography, and unauthorised access of a victim's phone/media. From our analysis, we identified three script tracks and constructed three distinct crime scripts: (1) threats, sextortion and dissemination; (2) unauthorised access of a victim's mobile device and dissemination; and (3) covert intimate filming. We highlight areas for potential intervention for law enforcement agencies and policy makers to increase deterrence and personal security in online and offline spaces.

Conclusion: Adult RS-IBSA occurs in a range of dating and domestic contexts. This study develops crime scripts for adult RS-IBSA and advances our understanding of how the Internet/smartphones/digital media translates into virtual crime scenes with opportunities for maximum harm infliction. We offer several policy implications including revising current RS-IBSA legislation and supporting law enforcement agencies with policing online and offline intimate relationship spaces through situational prevention.

Keywords: Retribution-style image-based sexual abuse, Cyber-enabled crime, Rational choice, Crime script analysis, Situational crime prevention

Introduction

The Information Age facilitates human interconnectivity and interactions but also increases the repertoire of tools and opportunities for intimate partner violence offending (Dragiewicz et al. 2018). This includes adult retribution-style image-based sexual abuse (RS-IBSA), defined by Powell et al. (2018) as "relationship retribution, where revenge is a motivation within the context of a current or past intimate relationship" (p. 393–394).

An analysis of the database of MyEx.com, a revenge pornography website revealed an approximation of 9285 posts created in the United States, 796 in the United Kingdom, 496 in Canada, 214 in Australia and 22 in New Zealand (Hall and Hearn 2019). Uhl et al. (2018) conducted a content analysis of 134 non-consensual photos contained on seven different websites which may not function specifically for the purpose

*Correspondence: acadresearch.oac@gmail.com; l.mazerolle@uq.edu.au
[1] School of Social Science, The University of Queensland, Brisbane, QLD 4072, Australia
Full list of author information is available at the end of the article

of hosting or promoting "revenge porn" or explicitly harming victims. Their study revealed that 92% of victims depicted in the images were women and that more than a third of the images had texts accompanying them which explained the perpetrator's reasons for sharing the women's image with the most common being that she was an "ex" (22%), "hot" or "sexy" (22%), "a slut" (15%), or unfaithful (6%). An international study of the extent and nature of IBSA in a community sample of Australian residents (n = 4053) aged 16 to 49 years by Powell et al. (2019) found that 1 in 10 participants engaged in IBSA perpetration behaviours such as the non-consensual taking of intimate images of another individual or threatening to disseminate or disseminating the images. A US-based study by Ruvalcaba and Eaton (2020) on RS-IBSA (n = 3044, 54% women) revealed that one in 12 participants experienced victimisation, one in 20 reported perpetration and women reported higher rates of victimisation and lower rates of perpetration than men. Women also experienced lower psychological well-being and higher somatic symptoms than non-female adult victims and higher somatic symptoms than adult male victims. The harms of adult RS-IBSA victimisation include unemployment, physical and online stalking, harassment, prolonged harms from images being retained and circulated on the Internet/third party digital tools (Bates 2017; Stroud 2014) and similar negative mental health effects as sexual assault (see Bates 2017).

A systematic review by Dehghanniri and Borrion (2019) of crime types covered by 105 crime scripts (a concept elaborated in the next section) from 1994 to 2018 revealed that the highest number of crime scripts have been constructed for cybercrime, followed by corruption and fraud offences, robbery and theft offences, and the lowest number for sexual offences. Unlike the more extensive crime scripting of pure cybercrime/cyber-focused crime (where the targets are data, computers, networks or similar) and traditional crime in the offline world, crime scripting of cyber-enabled/technology-facilitated/cyber-dependent crime is scant, as is scripting of cyber-enabled/technology-facilitated/cyber-dependent sexual crime. This is problematic as the line between traditional (physical) and online offending is becoming increasingly blurred (Bluett-Boyd et al. 2013; Reed et al. 2016) and criminal investigations and prosecutions are becoming highly reliant on reliable and credible digital evidence that can be used in court. Moreover, unlike traditional personal crimes such as physical and sexual assault, cyber-enabled personal crimes are characterised by technical competency (Yar 2005), trans-territoriality (Baym 2015) and high concealment (Pittaro 2007; Vitis 2020).

Cyber-enabled dating/domestic/sexual violence have been coined "hidden crimes" (Cook 1997, p. 127) and are therefore more susceptible to being under-reported and under-recorded (Cook 1997). Hatcher et al. (1999, p. 397, 399) contend that the risks and costs of cyber-enabled offending is lower than those in traditional crime, while the benefits are higher. This is also problematic as crimes of this nature are said to surpass the current capacity of public and private regulators to control (Grabosky 2000; Hiller and Cohen 2002; Langlois and Slane 2017), along with the low probability of arrest and conviction (see Li 2014). These facts support the need to reduce concealability of RS-IBSA for law enforcement and legislative policy makers to ensure that offenders are held accountable for their crimes and victims can fairly access the criminal justice system. Like pure cybercrime offenders, a single RS-IBSA offender can offend in multiple places and at multiple times on as many target platforms as possible regardless of geographical location or spatial boundaries, and with far-reaching negative impacts for the victim (Woodlock 2017). Hence, crime scripting in this cyber-enabled space is important and timely. To our knowledge, no crime script has been developed for adult-to-adult image-based sexual abuse offending by former or current dating/domestic partners.

This study undertakes a crime script analysis of adult RS-IBSA. Drawing on 19 court transcripts involving 18 adult RS-IBSA offenders from court records in New Zealand, we apply a deductive thematic analysis to the court transcripts by focussing our analysis on RS-IBSA crime data at offence-levels. We identify four distinct adult RS-IBSA offence categories and three crime script tracks. We proceed to construct three micro-level crime scripts (through crime script analysis) based on the three crime script tracks identified, and propose crime intervention points for all eight stages of the crime scripts. Implications for prevention and future avenues for research are then discussed.

Background

A script is a "picture plus caption" (Abelson 1976, p. 34) of a predetermined or stereotyped sequence of events or actions necessary to achieve a goal in a particular situation (Schank and Abelson 1977). According to Abelson (1981), in order to begin a script, an individual must have a stable cognitive representation of the script, an evoking context for the script which needs to be self-presented or environmentally presented and the individual must enter the script. Utilising Abelson's (1976) cognitive psychological approach to scripts, Cornish (1994a, b) pioneered the application of a script-theoretical framework (crime script analysis) to represent the complete sequence of actions initiated prior to, during and after

the commission of a crime (crime-commission process). Crime script analysis deconstructs crimes into chronological stages to identify "actionable offender decision points" (Wortley 2014 in Haelterman 2016, p. 12). Crime scripts also capture the criminal actors' roles, props, and locations in a sequence of actions to identify offender behavioural routines at every stage of the crime-commission process (Borrion 2013). Crime script analysis helps us understand the crime-commission process utilised by offenders to commit a specific crime by (1) extracting the offender's decision-making (rationale) and offending behaviour (Beauregard and Martineau 2015; Lavorgna 2015; Lord and Levi 2017; Meyer et al. 2015; Wortley and Mazerolle 2013), and (2) organising prior knowledge about the prerequisites of a crime-commission process such as the resources and skills required by offenders in order to successfully execute their crimes in a given situation (Balemba and Beauregard 2013; Bichler et al. 2013; Cornish 1994b; De Vries 2013).

Rational choice perspective

The rational choice perspective is a conceptual framework for understanding crime events and directing situational prevention initiatives. It explains how individuals consciously and rationally choose to commit criminal acts. Clarke and Cornish (1983, 1986, 2006) posit that potential offenders make deliberate and goal-directed decisions that maximise personal benefits and minimise personal costs (e.g., risk of apprehension) when choosing to commit and while committing a crime. Clarke and Cornish (1983) outlined that decisions to commit crimes need not be completely rational or carefully calibrated due to the constraints/circumstances under which these decisions are being made: criminals exercise bounded rationality (Einstadter and Henry 2006). For instance, offenders' decisions may be influenced by cognitive biases, time constraints, alcohol/drug use, heightened emotional states or prior learning models (Cornish and Clarke 2008). Additionally, offenders vary in their perceptions, attitudes, motivations, skills and abilities to analyse a situation and conduct choice structuring in weighing the benefits (rewards) versus costs (risks or efforts) in order to achieve favourable outcomes (Cornish and Clarke 1987). Offenders' goals also interact with and are modified according to situational factors such as the opportunities and incentives in the immediate environment (Cornish and Clarke 2008).

Hence, regardless of the crime category, offenders are considered fundamentally "rational" in their decision-making and perpetrate in order to attain their goals or satisfy their needs or desires such as money, power, control, revenge or sexual gratification, in the context of above (see Brantingham and Brantingham 1978; Clarke and Cornish 1985; Cusson 1983; Walsh 1978). When the rational choice perspective is applied to Cornish's (1994a, b) crime script framework, at each crime script stage, the offender is expected to make rational choices about how to optimally proceed to the next stage, and with successful replication, the script eventually develops into the default behavioural sequence until the crime is completed (Leclerc and Wortley 2014a, b).

Crime scripts as an outgrowth from the rational choice perspective

Cornish's (1994a, b) crime script analysis was also intended for situational crime prevention purposes—to help criminologists identify intervention points and tactical suggestions for intervention across crime types (Cornish and Clarke 2008). More specifically, Freilich and Chermak (2009) demonstrated how crime scripts outline opportunities for disrupting/altering the outcome and indicate precisely at what stage(s) in the crime-commission process (prior to, during, and/or after the crime) strategies could be utilised to prevent such crime events.

Application of crime scripts

Crime scripts were initially applied to property crimes such as robbery, automobile theft and vandalism (Cornish 1994a, b), the resale of stolen vehicles (Tremblay et al. 2001), burglary (Cornish and Clarke 2008; Nee and Meenaghan 2006) and theft of electronic products (Ekblom and Sidebottom 2008). Crime scripts have also been utilised on cybercrimes such as account takeover (Haelterman 2016), mapping trolling on a cyber-attack journey (Somer et al. 2018) and employee computer crime (Willison and Siponen 2009). In addition, crime scripts have helped explain the crime-commission process of sexual offences including adult-to-child sexual abuse (Deslauriers-Varin and Beauregard 2010; Leclerc 2013a; Leclerc et al. 2011); child sex trafficking (Brayley et al. 2011); compensated dating (Li 2015); human trafficking for sexual exploitation (Savona et al. 2014); sex offenders (Beauregard et al. 2007); sexual offences (Cook et al. 2019); stranger rape against women (Chiu and Leclerc 2017); acquaintance rape against women (Chiu and Leclerc 2017) and Internet-mediated sex trafficking (Lavorgna 2014). The application of crime scripts across different crime categories demonstrates that they are not only appropriate for describing the crime-commission process of physical (traditional crime) but also cyber-dependent and cyber-enabled crime.

Crime script levels

Although crime scripts present the procedural sequence of a crime-commission process, Cornish (1994a, b) proposed different crime script levels of abstraction: *tracks*,

scripts, *protoscripts* and *metascripts*. The highest (macro-level) of abstraction is the *metascript* which represents the generalisation of subgroups of an offence, such as "property theft" and "sexual offending". The upper meso-level of abstraction is the *protoscript* whereby a specific crime is generalised such as "robbery from the person" and "sexual abuse of male children" respectively. The lower-meso level is the *script* which refers to specific offences that are subdivided by dimensions (broken down into stages/acts/scenes) within a given situation (Leclerc et al. 2010).

The lowest (micro-level) is the *track* which is most commonly used in situational crime prevention (Leclerc et al. 2011). It describes the different routes that are available through acts and scenes of a specific crime taking place in a specific setting such as "subway mugging" and the "sexual abuse of male children in a particular setting" in a school/household. Cornish (1994a) after Leddo and Abelson (1986) and Ekblom; quoted in Cornish (1994a: 161), established a "universal script" including the generic structure of scripts which includes eight script scenes/functions: *"Preparation, Entry, Preconditions, Initiation, Actualisation, Doing, Post-condition* and *Exit".* Tompson and Chainey (2011), who refuted the notion of pre- and post-conditions being distinct and separate scenes, reduced the script to four categories and emphasised the importance of the requirements and facilitators within each scene. Although some researchers have argued that the eight script scenes' generic structure is challenging to apply in practice (Ekblom and Gill 2015), others assert that there needs to be a balance between appropriate levels of generalisation to allow for the exploration of meaningful variations in scripts (Wortley in Ekblom and Gill 2015). We took this into consideration when selecting a suitable crime script framework to guide the construction of adult RS-IBSA crime scripts.

Aims and objectives of the study

To understand and explain the crime-commission process of adult RS-IBSA by former or current dating/sexual/domestic partners, we needed to understand the different *tracks* of RS-IBSA offending in various situational contexts. In order to do this, it was necessary to source for relevant crime scripts involving "personal" crime with a strong component of "abuse" and ensure that the "sexual" setting(s) used in these crime scripts was/were comparable (Appendix 1). We identified two separate sexual abuse (offending) studies which utilised crime scripts (Chiu and Leclerc 2017; Leclerc et al. 2011) to guide our development of RS-IBSA crime scripts. In order to identify as many offending *tracks* for RS-IBSA as possible, we used the data categorisation table in Chiu and Leclerc's (2017) study for the examination of sexual offences against women by acquaintances (Appendix 2). Understanding the *tracks* helped us develop crime scripts for RS-IBSA. Although we used Chiu and Leclerc's (2017) data categorisation table to examine various *tracks* in RS-IBSA, we discovered that the sequence of crime variables for RS-IBSA were incongruous with the sequence of crime variables situated in the crime script devised by these researchers (Appendix 3). We refer specifically to the crime variables used in their *Instrumental Actualisation*, *Offender Approach Method* and *Continuation* script stages. To overcome this challenge in our crime script development process, we employed an older but more flexible crime script devised by Leclerc et al. (2011, p. 221) for child sexual abuse which allowed for more exploration of RS-IBSA and we incorporated these crime stages/scenes into our RS-IBSA crime scripts: *entry to setting*, *instrumental initiation*, *instrumental initiation (continuation) I*, *instrumental initiation (continuation) II*, *instrumental actualisation*, *completion*, *outcomes* and *post condition* (Appendix 4). Notably, this crime script by Leclerc et al. (2011) delved deeper into the modus operandi/abuse which is integral to RS-IBSA offending. We included an additional stage, *offender-victim prehistory* from Chiu and Leclerc's (2017) crime script for sexual offences against women by acquaintances to provide contextual background to the RS-IBSA offending types.

Data and methods

Research site

According to the District Court of New Zealand, it is the largest court in Australasia (https://www.districtcourts.govt.nz/). The majority of New Zealanders who take legal action or have had legal action taken against them are required to undergo the entire justice process in the District Court (including four court divisions: criminal, civil, family and youth courts). *The District Court of New Zealand* website publishes a representative sample of cases which outline important judicial decisions of government priority and public interest. The published selections featured on their website are updated regularly in an independent process which is overseen by an Editorial Board of judges. New Zealand aims to improve the openness and transparency of justice administration by allowing the public to access these court publications in addition to other legal background information. Real names have been omitted from the publications and substituted with pseudonyms including in areas where there is a possibility that the protected party/parties may be identified.

Our data collection phase took place from 2 July 2018 to 2 September 2019. To begin the process of narrowing down our online search (see Appendix 1), we input "Harmful Digital Communications" in the filter search bar on *The District Court of New Zealand* website to

focus on cases linked to the Harmful Digital Communications Act (2015, http://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html). This enabled us to only view the publications involving harmful digital communications (n = 83). We proceeded to remove all regulatory documents (n = 17) until we were only left with court transcripts (n = 66). We removed family and civil court transcripts (n = 3) and all duplicate court transcripts (n = 13). Only court transcripts that were tagged as "Criminal" (n = 41) were then considered for this study and assessed further for eligibility.

To identify IBSA court transcripts involving only the misuse of a victim's intimate images by former and/or current dating and/or domestic partners (separated or otherwise), we proceeded to read all the 41 criminal court summaries and full court transcripts and checked for eligibility based on key words and terminology indicating the misuse of intimate images (e.g., naked images/videos). We then proceeded to examine each court transcript for the ages of victims and offenders and their relationship dynamics to identify only adult (over 18 years of age) RS-IBSA cases for the development of crime scripts. We excluded all other types of technology-facilitated coercive control (such as abusive language, verbal threats, harassment, hacking, covert surveillance) and other criminal offences (such as drug and alcohol-related offences, physical assault). IBSA perpetrated by acquaintances with no prior romantic or sexual relationship with the victim, IBSA perpetrated by a paid customer to a commercial sex worker, technology-facilitated sexual offences perpetrated by adults involving minors (under 16 years of age) and child sexual exploitation material cases were also excluded as these do not fall under the typology of adult RS-IBSA. In total, we deemed 26 cases to be ineligible through this screening process (Fig. 1).

Sample and data sources

We used all 19 eligible court transcripts that included adult RS-IBSA offenders (n = 18) from years 2015–2018 that were publicly released on The District Court of New Zealand's court record database under the search category of *Harmful Digital Communications*. We utilised 19 court transcripts for 18 offenders. The additional court transcript was due to one offender attending two court hearings which were transcribed and then uploaded onto the database on two separate occasions. Court transcripts that did not explicitly reference a victim's intimate images being used in the adult RS-IBSA offending were excluded.

In our sample of 18 offenders, 17 were male and one was female. We had missing data for the ages of 10 offenders but all offenders attending criminal court by New Zealand law are aged 18 years and above. Eight offenders already had a criminal record prior to their court trials, and 10 with no prior criminal history were on trial for other offences in addition to RS-IBSA. Only one offender was identified as Australian whilst the remaining 17 presumably possess New Zealand citizenship as this was not highlighted anywhere in the judicial sentencing reports. The RS-IBSA offender-victim relationship type was formerly dating (n = 8); domestic relationship (n = 5); married but separated (n = 2); former online and offline casual (sexual) relationship (n = 1); and currently dating (n = 2). The duration of these relationships spanned between several months and 10 years but we could not account for the duration of all relationships as this information was not provided in 11 court transcripts. As some cases involved more than one RS-IBSA offence, the crime script may vary from one offence to the other for the same offenders.

Descriptive statistics: measures of frequency

The temporal offending patterns of RS-IBSA offending included one occasion/day (n = 11); two occasions/days (n = 2); three occasions/days (n = 4); and four or more occasions (n = 1) which took place over a 22-month period. Consistent with previous literature (DeKeseredy and Schwartz 2016; McGlynn et al. 2017; Powell and Henry 2017), the RS-IBSA offences in this sample included the non-consensual dissemination of a victim's intimate images (videos and/or photography, n = 16); sexual exploitation (n = 2); non-consensual photography (n = 1); doxing (n = 5); and threats to disseminate a victim's intimate images (n = 21). We investigated *threats* in this study to understand the frequency and efficacy when employed in different RS-IBSA offending types. For instance, one offender resorted to "credible" threats to disseminate his victim's intimate images resulting in the sexual exploitation of his victim. Another offender was caught by the police before he disseminated his victim's intimate images.

Although *doxing*, "the intentional public release onto the Internet of personal information about an individual by a third party, often with the intent to humiliate, threaten, intimidate, or punish the identified individual" (Douglas 2016, p. 199) by definition does not include the non-consensual dissemination of an individual's intimate images, the five offenders in this sample who *doxed* their victims attached their victims' private or identifying information to their victim's intimate images with the intention to maximise harm. Investigating *doxing* enables us to understand the severity of offending in different script tracks. Fourteen offenders used intimate photographs/pictures of their victims in their offending, four offenders used videos of their victims engaging in various independent sexual

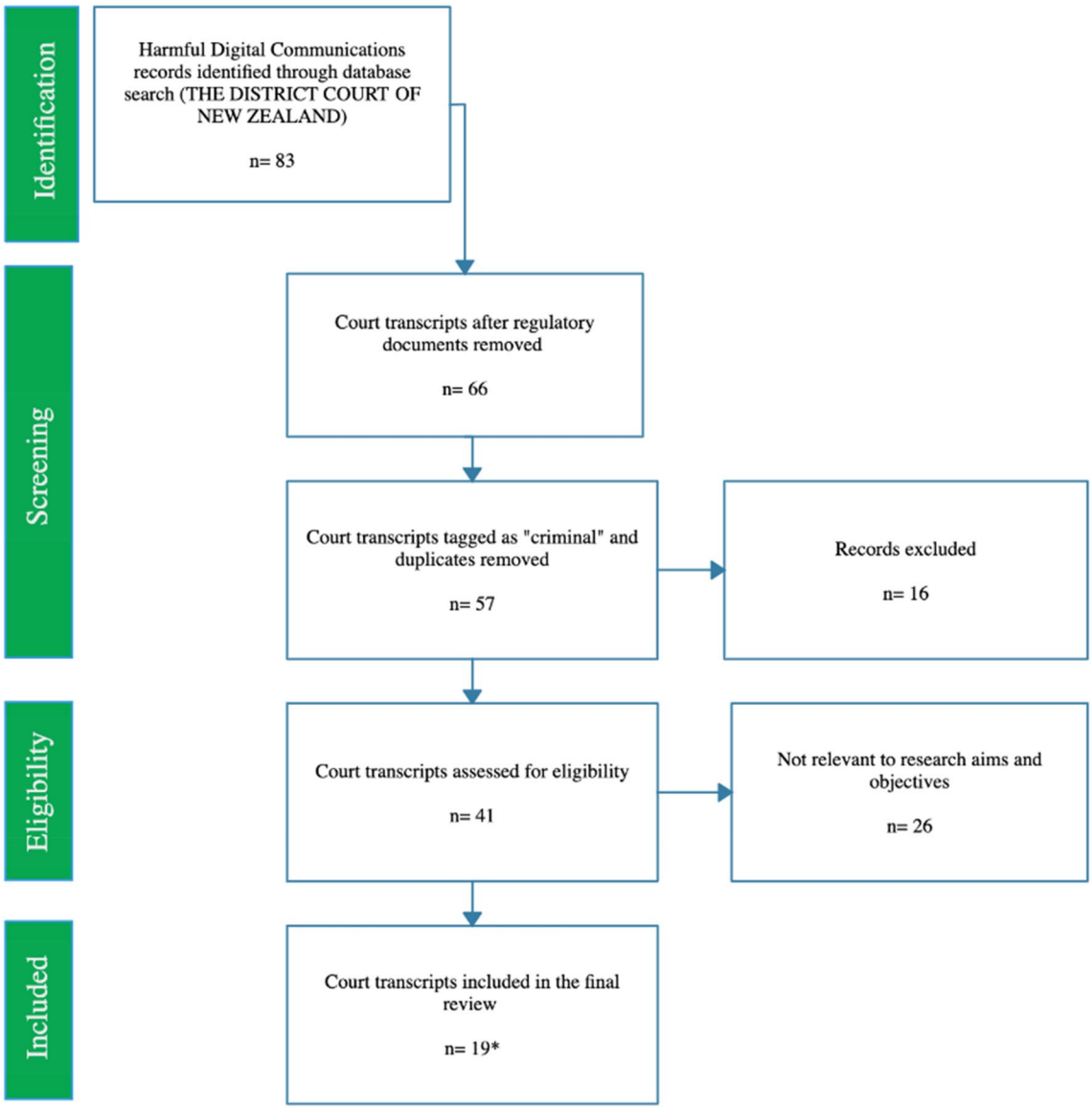

Fig. 1 The Preferred Reporting Items for Systematic Reviews and Meta-analyses (PRISMA) model. 19 court transcripts for 18 offenders

acts, sexual acts with the offender or sexual acts with a third party, and one offender used a combination of one intimate photograph (close-up of female victim's genitals with her face) and three sexual videos. All intimate images featured females and their body parts with one exception. Offenders disseminated their victim's intimate images through three channels: public (n = 8), friends and family (n = 7) and/or the victim directly (n = 4). The platforms used included Facebook (FB) Messenger (n = 2); victim's personal FB page (n = 6); FB public page (n = 8); a pornographic site (n = 1); email (n = 3); work-based web page (n = 1); and a website of a corporation (n = 1).

According to Porter (2008), archival court data cites multiple sources of evidence such as offender, witness and victim statements and forensic evidence. Collectively, these have been subject to strict legal examination or fact checking. As these open-source court data are easily accessible to the public, this suggests that care has been taken by the Courts to maintain confidentiality of protected parties, namely adult RS-IBSA victims. We demonstrate through this research the usefulness, ease and affordability of this secondary data source in helping us establish an evidence base for the crime-commission process of adult RS-IBSA and proposing steps towards prevention.

Analytic strategy

To achieve our research objectives on adult RS-IBSA, we partially replicated the analytical strategy, otherwise known as a script analysis process, in Chiu and Leclerc's (2017) study which examined sexual offences against women by acquaintances using a script framework for prevention purposes. Given the uniqueness of each court case, the preliminary stages of our research, and no prior crime scripts being constructed on adult RS-IBSA in existing literature, we approached the development of the adult RS-IBSA crime scripts using the offence-level of analysis. However, before we could proceed with this, we conducted a thematic analysis (in place of the content analysis used in Chiu and Leclerc 2017) on all 19 court transcripts for the 18 offender profiles. We coded for unit(s) of meaning (i.e., RS-IBSA offences) and categories for individual crime variables and sub-categories of crime variables: *Social elements*, *Approach Method*, *Setting*, *Interaction*, and *Other variables* (Chiu and Leclerc 2017). We also tabulated the total number, frequency and severity of adult RS-IBSA offences in order to identify different styles of adult RS-IBSA offending and situate specific adult RS-IBSA offences in the appropriate stage(s) of each crime script.

Specifically, we proceeded to execute the analytical strategy for script development in this sequence: (1) extracting all relevant crime data (e.g., identifying only adult RS-IBSA offences; frequency and severity of adult RS-IBSA offences; sequence of actions leading up to the adult RS-IBSA offending drawing from legal facts, words, phrases and/or sentences used by the judges); (2) coding and tabulating the types and number of adult RS-IBSA offences in all 18 court transcripts; (3) matching these offences to individual and sub-categories of crime variables in the data categorisation table constructed by Chiu and Leclerc (2017); (4) checking the completed data categorisation table for repetition and overlaps, and making revisions where necessary; (5) scanning the completed data categorisation table for common crime patterns and points and comparing them in order to identify distinct types of adult RS-IBSA script tracks; (6) constructing one or more draft crime scripts using Chiu and Leclerc's (2017) final crime script draft for sexual offenses against women by acquaintances whilst toggling back and forth between the data categorisation table and the original court summaries to ensure fit and accuracy; and (7) refining the final crime script(s) (see also Chiu and Leclerc 2017; Chiu et al. 2011).

Results

We identified four categories of adult RS-IBSA acts: (1) non-consensual dissemination of a victim's intimate images with or without threats; (2) violent cyber sextortion (monetary or sexual gain); (3) covert intimate photography; and (4) unauthorised access of a victim's phone/media and disseminating a victim's intimate images from the victim's account(s). From our thematic analysis, we identified three script tracks and constructed three distinct crime scripts for (1) threats, sextortion and dissemination; (2) unauthorised access of a victim's mobile device and dissemination; and (3) covert intimate filming.

Script tracks differed based on relationship type: dating and casual sexual relationships tended to result in the dissemination of a victim's intimate images publicly whilst domestic relationships and marriages (with spouses separated) tended to result in dissemination to the victim's employers/potential employers and to the victim's friends and/or family.

Crime script analysis of court transcripts

To date, no crime script analysis has been undertaken on RS-IBSA. As the research was exploratory, we could not predict the number of scripts from our sample of RS-IBSA offenders before completing the analysis. The discovery of multiple script tracks led us to conclude that three crime scripts, rather than a single crime script, was necessary to encompass all the findings. Compiling everything into a single crime script would have reduced specificity and jeopardised the accuracy of the findings.

By constructing more than one crime script, we were able to address potential terminology or definitional issues in a way that was easier to interpret than what would have been the case with more complex scenes in each script. This aligns with our emphasis on a more systematic and standardised crime scripting technique for RS-IBSA—a complex and multi-faceted "non-traditional" personal crime which is highly variable and dependent on the "situational" context in intimate relationship spaces and in online/offline spaces.

Based on the data categorisation of adult RS-IBSA court transcripts (Table 1), we identified three RS-IBSA script tracks and constructed three crime scripts for each offending style: threats, sextortion and dissemination (Fig. 2), unauthorised access of victim's mobile device and dissemination (Fig. 3), and covert intimate filming (Fig. 4). The generic offender prehistory will be presented prior to the three crime scripts.

Offender-victim prehistory

The thematic analysis conducted on the court transcripts revealed that adult RS-IBSA occurs frequently in the context of a relationship breakdown which is consistent with previous research. According to Kelly and Johnson (2008), separation can be perceived as a provocation and a threat to the abusive partner's (offender's) power and

Table 1 Data categorisation from adult RS-IBSA court transcripts (n = 19)

Variables	Categories
Social elements	
Actors involved	Offender; victim; third parties (victim's child, offender's and victim's child, extramarital partner, victim's parent, third party engaging in sex with the victim, male peers)
Relationship between victim and offender	Committed partner, sexual partner, cheating partner (see Drouin et al. 2013); former sexual relationship; former dating partner; current dating partner; former domestic partner; current domestic partner; married; separated; in the process of separating; victim's parent; mother-daughter; ex-partner-mother (victim's) biological son; mother (offender)
Circumstances	Dating/domestic relationship/marriage breakdown; victim initiates break-up; victim refuses to get back together; victim refuses to accept break-up initiated by offender; victim refuses to communicate with offender after break-up; victim takes action to have intimate photos taken down from sites; victim requests photos to be deleted on offender's mobile device; extramarital affairs; victim does not find offender's threats credible; victim refuses to pay sum of money to offender; victim does not know offender is in possession of intimate pictures/videos; victim sent offender images during online interactions before formalising offline domestic/sexual relationship
Approach method	
Confrontation	Offender wanted to get back together with victim; wanted to get victim to stop seeing new partner; wanted to turn daughter against her father; initiated break-up and moved on to date victim's friend; threatened to disseminate images if victim did not stop contacting him; installed tracking app on mobile device; unauthorised access of victim's unattended smartphone/computer/email/Facebook accounts; changed passwords; uploaded victim's images from victim's social media account
Surprise	Offender possesses/still possesses victim's images and/or has kept images not withstanding victim's constant requests that the offender deletes them; non-consensual photography; intimate covert filming; consensually taken images disseminated without warning; breach of trust; sending victim's images to victim as proof that they are still in possession of the victim's images and are not afraid to post them publicly or to friends and family
Blitz	Used victim's intimate images (taken with victim's consent and/or without victim's consent); victim's face fully identifiable in nude/semi-nude images; close-up images of victim's genitalia and intimate visual recordings of victim engaging in sexual acts such as masturbation, oral sex and sexual intercourse; exploiting digital communications technologies and poor regulation of social media platforms; pornographic sites; victim leaving smartphone and computer unattended; victim not logging out of social media accounts on smartphone; knowing the victim's social connections and how best to inflict harm on them through selectively targeting recipients (public, friends and family or victim directly); blackmail with or without a sum of money
Setting	
Location	Pornography sites; social media public groups catering to men seeking sexual services; work-based website; social media pages; a website of a corporation; smartphones; Facebook messenger; victim's social media account; email; threats to post during physical meetings and via text messages; physical setting where victim was covertly filmed/photographed (with or without consent)
More than one crime scene	Yes/no
Time	Daylight; darkness
Interaction	
Victim reaction	Resisted; ignored offender; stayed in relationship with offender out of fear; complied to sexual requests out of fear; initiated steps to get images taken down from websites; sought legal help and intermediary services; filed police report
Offender reaction	Used threats; ignored victim's pleas not to disclose images; refused to delete victim's intimate images; blackmail; negotiation; ceased to demand anything from victim; posted image on victim's social media account Timeline (private settings) or sent image via instant messenger (IM) to victim's family (e.g., son or daughter—can be minors, mother, etc.); repeated uploading of intimate visual recordings; bypassed threats
RS-IBSA acts	Disclosing content to a specific target audience (victim's closest family or friends, usually 1–2 individuals); disclosing content to a larger audience (victim's friends or public) using multiple platforms; disclosing personal information such as direct reference to name, mobile phone number, e-mail; attaching a price tag of "$1" to each image; advertising victim's body for sexual services (e.g., "She's DTF boys"); disclosing victim's intimate video recordings on pornographic site; offensive labelling of images or video footage (e.g., "Dirty whore" and "Slut begs for it in the arse")
Other variables	
Disruption	Third party intervened/disrupted (friend of victim and witness during trial); victim sought help from police before images were posted; police investigating offender for other charges; offender (wife) tried to undo damage on victim (husband) and their child by confessing to lawyers and the police her unauthorised access of husband's smartphone and FB account; changing passwords and disseminating intimate images using FB account
Exit	Offender stops contacting victim; victim stops contacting offender
Threats/force	No threats with immediate action; threats used (1-12 threats); threats severe enough to elicit victim compliance with sexual requests by offender and/or relationship continuation with offender; doxing to inflict the most harm on victim

Table 1 (continued)

Variables	Categories
Tools/transport	iPhone with camera and image storage folder; smartphone with social media applications downloaded; smartphone with IM software downloaded (WhatsApp and FB Messenger); victim's address book; victim's browser history; pornography sites; email; work-based sites; social media (FB) public groups; privacy settings; tagging option; public groups catering to men seeking sexual services; smartphones left unattended by victim; passwords given to offender by victim; creating new social media account; websites and other digital (including social media) platforms allowing uploads of nude and semi-nude photographs; sexual videos and advertising for sexual services and with poor regulation policies for IBSA offences
Post-action	Tried to comfort victim/be intimate with victim; concealed circumstances from police
Other	Potential "triggers" (date/sexual advance rejection, prior relationship break-up); prior alcohol and drug problems or convictions (e.g., driving dangerously or driving with excess breath alcohol, possession of drugs); prior history of domestic violence or convictions (e.g., male assaults female, breach of protection order); mental health problems (e.g., self-harm, substance abuse/addiction)

The term *trigger* refers to factors or offender-victim prehistory that may result in the offender being in a heightened emotional state (e.g., stress/anger), and is not intended to imply causality. In some legal cases, the victim is the recipient of intimate images (e.g., Offender #1; Offender #14; Offender #17). We substituted the variable *con* with *confrontation* to deconstruct and identify different script tracks for RS-IBSA. This is our only modification to the data categorisation table. Adapted from "Table 6.1. Data categorisation from court transcripts" by Chiu and Leclerc (2017)

control, and around the time of separation, acts of severe physical, sexual and emotional abuse, harassment, coercive controlling behaviours are likely to persist and even escalate (Crossman et al. 2016; Myhill 2015; Ornstein and Rickne 2013). Coercive control tactics documented in RS-IBSA offending include monitoring (covert surveillance/tracking of a victim's movements and activities); controlling the victim's actions (Pitman 2017; Velonis 2016); harassing the victim on the phone/computer/social media; pressuring or coercing the victim into remaining in an abusive relationship with them; and/or paying a sum of money or engaging in sexual acts (Dragiewicz et al. 2018; Draucker and Martsolf 2010; Melander 2010).

Offending was prevalent in all types of intimate relationships: dating relationships, casual sexual relationships, domestic partnerships, marriages whereby both parties were separated or separating, and extramarital partnerships. Offending was also present in short and long-term relationships (several months to 10 years). The majority of cases (n = 17) involved intimate images that were consensually taken by the victim and/or the offender and later shared without consent, but there was one case involving the offender ignoring the victim's requests to delete her intimate images from his smartphone, and another case involving covert intimate photography of the victim's body.

It was not uncommon for dating, domestic and spousal abuse (including prior assault convictions for males assaulting females, property damage, and breaching protection orders) to be present prior to the RS-IBSA offending. For example, an offender disseminated his current dating partner's (victim's) intimate images 2 days after he physically assaulted her. Another offender who covertly photographed his female victim and retained her intimate images without her consent already had 14 prior charges of making intimate visual photographs and publishing them. Prior and current alcohol and drug charges were also evident with six offenders, with some of these occurring during the offender-victim relationship and others before the relationship. However, prior criminality is not evident in all RS-IBSA offenders in this sample. Eleven offenders did not have any prior criminal convictions or other charges in addition to their RS-IBSA offending. Extramarital affairs (with the victim or the offender being unfaithful) triggering RS-IBSA were also identified in two cases. All RS-IBSA relationships started offline except for two cases whereby the victim shared her intimate images with the offender before meeting offline and then commencing an offline sexual relationship (Offender #5) and meeting on FB and then commencing an offline domestic relationship (Offender #9). Most of the offending was committed immediately post-break up (on one, two or three occasions) whilst two other cases evidenced prolonged periods of RS-IBSA offending with the victim not being able to severe ties with the offender (Offender #12 and Offender #5) due to credible threats.

Crime script stages for threats, sextortion and dissemination

1. **Entry to setting (circumstances, location, time, third parties)**
   The setting in which the victim is first encountered can be in physical and/or virtual space(s). In most cases, the setting involved various digital communications platforms: standard text message; social media accounts and instant messenger software (FB Messenger); the offender's own mobile device with stored intimate images (photographs/videos) of a former/current partner who consented to (1) sharing

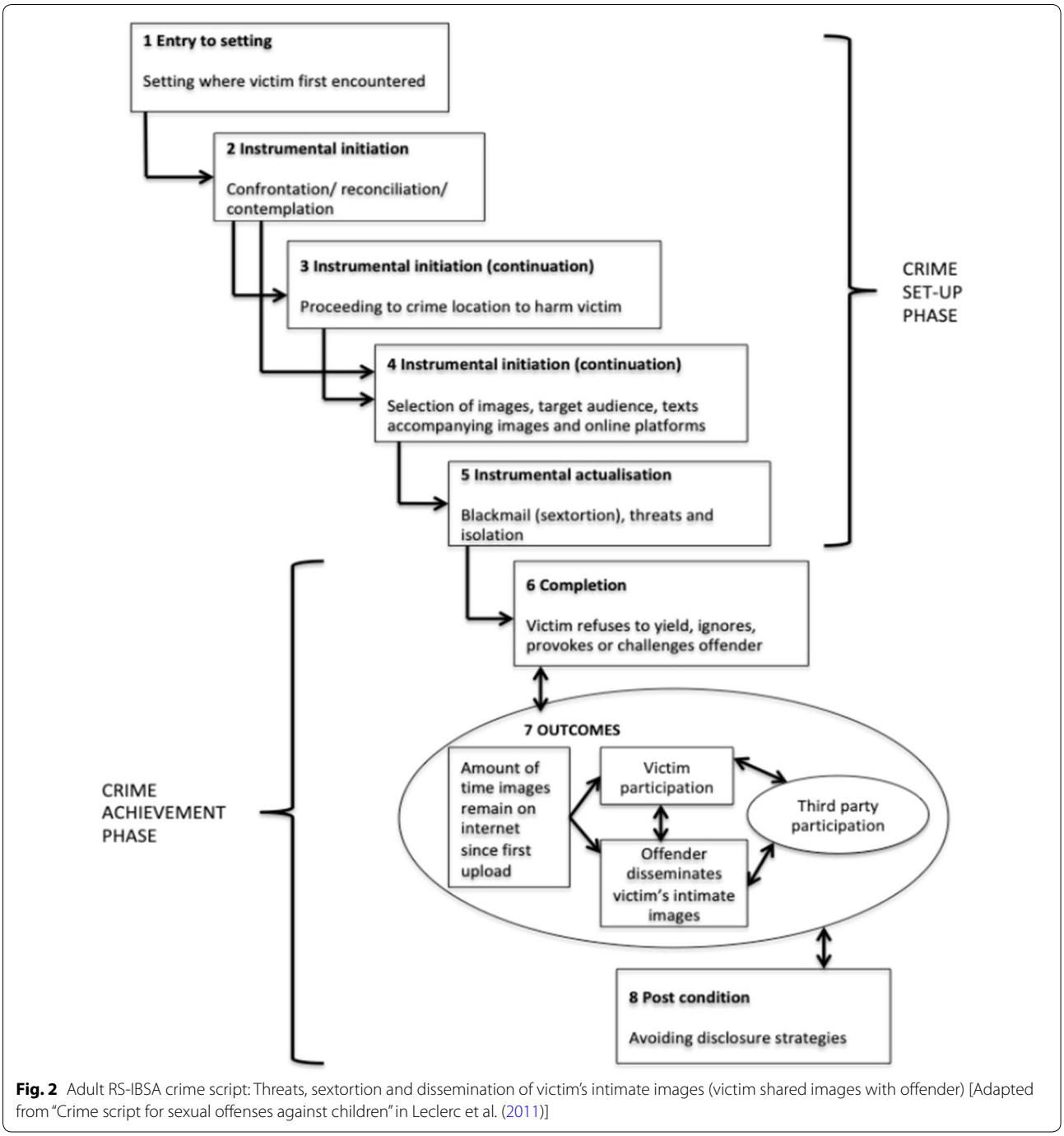

Fig. 2 Adult RS-IBSA crime script: Threats, sextortion and dissemination of victim's intimate images (victim shared images with offender) [Adapted from "Crime script for sexual offenses against children" in Leclerc et al. (2011)]

the images with the offender and/or (2) being photographed/filmed while naked/masturbating/engaging in sexual acts with the offender or a third party.

2. **Instrumental initiation**
   Confrontations were typically initiated by the offender (former or current intimate partner) with the purpose of repairing a broken relationship; getting in-touch with the victim while on a protection order; soliciting unwanted sexual favours and/or a sum of money from the victim; preparing to manipulate using credible threats to disseminate the victim's intimate images; regulating a former or current partner's relationships and activities or creating discord between parent and child. In one case, the victim

confronted the former partner (offender) about his initiation of a break-up and his decision to then date her friend. The offender retaliated with threats to disseminate her intimate images if she interfered in his new dating relationship. In other cases, there were no clear confrontations after the break-up or threats to disseminate a victim's intimate images and hence, this can be labelled as *contemplating* dissemination.

3. **Instrumental initiation (continuation) I**
   The offender proceeds to access the victim's intimate images stored on offender's smartphone.
4. **Instrumental initiation (continuation) II**
   The offender browses through his/her smartphone and selects the images to be disseminated, the target audience, text accompanying the images (e.g., derogatory and degrading texts, doxing) and which online platforms to use in the dissemination.
5. **Instrumental actualisation**
   The offender resorts to blackmail or sextortion, threats and isolating the victim. For example, Offender #5 who retained his victim's intimate images against her will, employed the compliance strategy of credible threats and succeeded in extorting sexual favours from her for a period of time.
6. **Completion**
   The victim refuses to yield to the offender's requests to communicate, pays the offender the demanded sum of money, ignores the offender's threats, or provokes or challenges the offender by taking steps to remove her intimate images from respective platforms to which they were uploaded.
7. **Outcomes**
   This refers to the amount of time the victim's intimate images remain on the Internet since the first upload, and third parties' reactions (e.g., downloading, storing, consuming, and disseminating images or contacting victim for sexual services).
8. **Post condition**
   Avoiding disclosure strategies involve the offender maintaining abusive contact with the victim and maximising psychological harm, reiterating to the victim that she fully consented to sharing her intimate images with the offender and/or to be photographed/filmed by the offender. Coercive control tactics such as threats and sexual entitlement were also successfully employed by an offender who was formerly in a casual sexual relationship with his victim in both online and offline spaces. Other cases evidence the offender attempting to reconcile with the victim after the offending, and conceal circumstances from the police.

Crime script stages for unauthorised accessing of victim's phone/media

1. **Entry to setting (circumstances, location, time, third parties)**
   The setting is the physical place where the victim leaves his/her mobile phone unattended and/or unlocked and stores their intimate images. This enables the offender to access the victim's images with little resistance.
2. **Instrumental initiation**
   This involves the planning phase before accessing a victim's mobile device and intimate image folder. The offender's activities may include manipulating the victim into leaving his/her mobile device unattended and/or unlocked or monitoring the victim's routine activities around his/her mobile phone storage and digital hygiene (online safety practices or lack thereof).
3. **Instrumental initiation (continuation) I**
   The offender proceeds to the physical setting where the victim is most likely to have left his/her mobile phone unattended/unlocked.
4. **Instrumental initiation (continuation) II**
   The offender waits for victim to abandon his/her mobile device.
5. **Instrumental actualisation**
   The offender accesses the victim's mobile device and browses image folders for intimate images. For example, Offender #12 installed a tracking application on the victim's smartphone without her authorisation, was able to directly access her email and social media account and contact the victim through these mediums, and target the appropriate recipient (victim's friend).
6. **Completion**
   The offender selects the victim's intimate image(s) to be disseminated, logs into victim's social media account and disseminates the images to the targeted recipient(s). For example, Offender #16 (wife) attached sexually aggressive text to the two image(s) of a man's genitals in a fully aroused state and then proceeded to disseminate these images to her daughter through the victim's (her husband's) FB messenger.
7. **Outcomes**
   This refers to the amount of time taken to access the intimate images; create texts and disclose image(s) to target audience; victim's unintentional participation (i.e., time away from their phone; leaving phone unlocked and social media account automatically logged in; victim sharing smartphone passwords with offender; victim not monitoring spikes in data

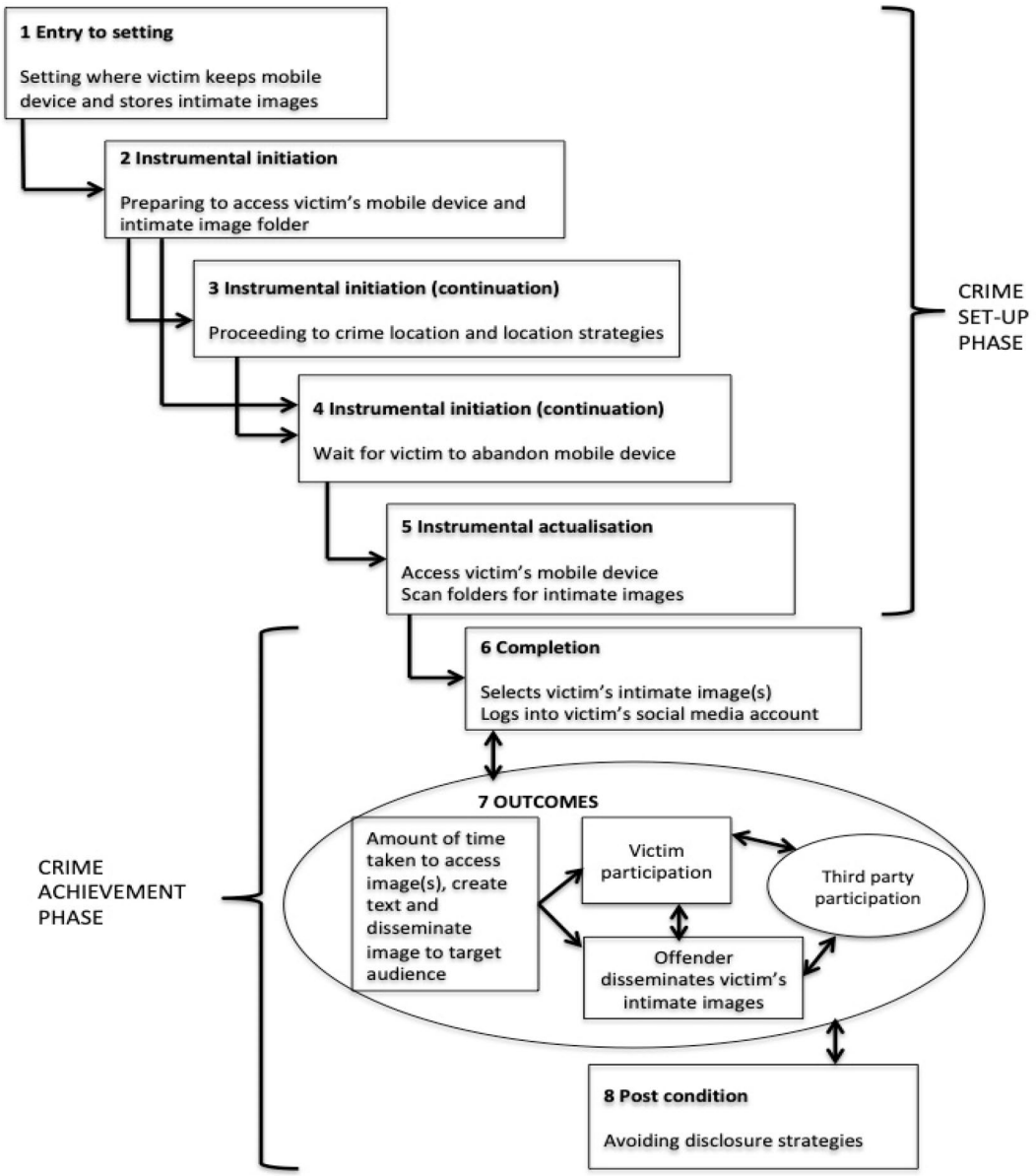

Fig. 3 Image-based sexual abuse crime script: unauthorised access of a victim's mobile device (victim does not disclose images to offender) [Adapted from "Crime script for sexual offenses against children" in Leclerc et al. (2011)]

charges; and third parties' reactions such as downloading, storing and consuming images, disseminating images or contacting victim for sexual services). For example, Offender #12 accessed the victim's smartphone and installed a tracking application with monitoring and control capabilities at a monthly subscription of US$14.95.

8. **Post condition**
   Avoiding disclosure strategies would be less complex if the offender successfully avoided detection by the victim (i.e., the victim was completely unaware that their smartphone, email and social media accounts had been accessed or a tracking app had been installed by the offender).

Crime script stages for intimate covert filming/photography

1. **Entry to setting (circumstances, location, time, third parties)**
   This can be a physical and private location such as the bathroom or bedroom. The victim may be present or absent.

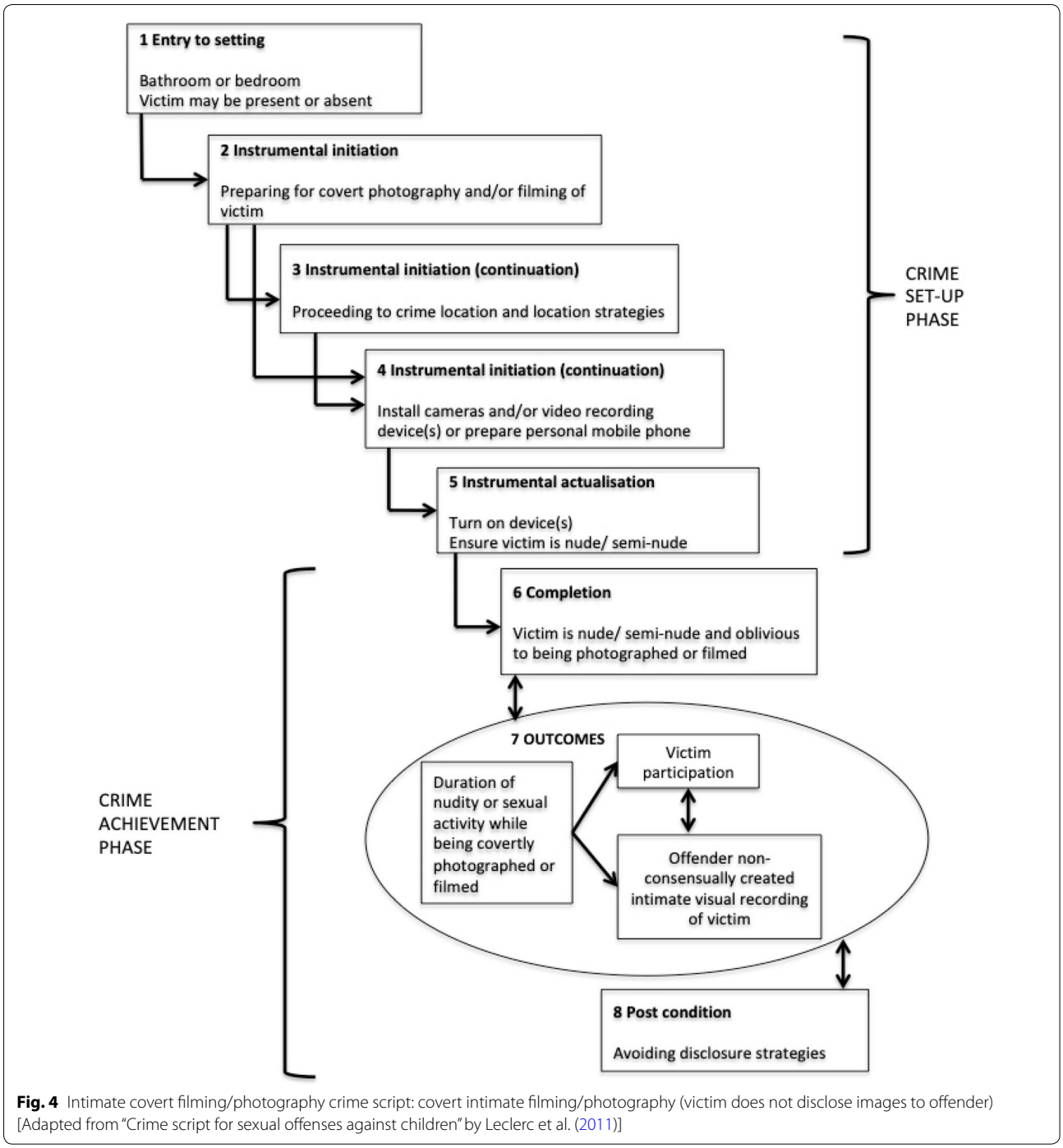

Fig. 4 Intimate covert filming/photography crime script: covert intimate filming/photography (victim does not disclose images to offender) [Adapted from "Crime script for sexual offenses against children" by Leclerc et al. (2011)]

2. **Instrumental initiation**
   This involves the preparation for covert photography or filming of the victim naked and/or engaged in various sexual acts in the bathroom and/or bedroom.
3. **Instrumental initiation (continuation) I**
   If the victim is present in the bathroom or bedroom, the offender would plan where and how to best capture the victim in nude and/or sexual positions without the victim's knowledge.
4. **Instrumental initiation (continuation) II**
   The offender installs cameras and/or video recording device(s), accesses camera function on mobile phone.
5. **Instrumental actualisation**
   The offender turns on the recording device and ensures victim is nude/semi-nude and/or engaging in sexual activity.

6. **Completion**
   The victim is nude/semi-nude and/or is engaging in sexual activity and oblivious to being photographed or filmed.
7. **Outcomes**
   This refers to the duration of nudity and/or sexual activity while being photographed or filmed, the victim's unintentional participation (i.e., the victim being unaware that she/he is being filmed) and the offender's non-consensual creation of intimate visual recording(s) of the victim.
8. **Post condition**
   Avoiding disclosure strategies would be less complex if the offender was not suspected by the victim or if the offender stored these covert intimate visual recordings surreptitiously.

Discussion

Unlike crime scripting of traditional (physical) and pure cybercrimes, crime scripts for cyber-enabled/technology-facilitated crime is scant. With more physical and sexual abuse offenders "rationally" perpetrating their crimes in online spaces, we acknowledged the necessity of crime scripts for RS-IBSA to facilitate criminal investigations and prosecutions which rely heavily on digital evidence. The crime scripts we devised for adult RS-IBSA are also targeted at crime prevention.

We documented actual examples of the displacement of offline dating/domestic and sexual crimes into online/digital spaces. Moreover, while cybercrimes are sometimes juxtaposed to offline crimes as distinct categories, we demonstrate that online and offline elements of RS-IBSA in the cases analysed were not mutually exclusive or discrete, but rather overlapping and dependent on one another: there was an interplay of online and offline aspects that demonstrates how these are interconnected. For example in relation to Fig. 2, in order to overcome police protection orders, one adult RS-IBSA offender resorted to initiating/demanding contact with the victim through threats to disseminate the victim's intimate images (Offender #6) while another proceeded to disseminate the images without prior contact/threats and concealing the origin of digital evidence (Offender #14). Another case involved a victim continuing an offline relationship with the offender against her will due to credible threats to disseminate her intimate images online (Offender #12). We also document a case of an offender disseminating a victim's intimate images when the offender became aware of the victim's successes with takedown requests (Offender #16).

Sexual abuse in adult RS-IBSA is also evidenced through the soliciting of sexual favours (Offender #5) and money (Offender #11). Sexual abuse is also demonstrated when the offender endangers a victim's personal safety through *doxing* (publicising the victim's personal information to males seeking sexual services and selling her intimate images). These RS-IBSA acts directly expose the victim to stranger and acquaintance stalking, harassment and rape. However, we did not document any RS-IBSA offending which involved the offender photographing/filming a current/former intimate partner (victim) being raped and/or sexually assaulted. Lastly, offending tools differ based on relationship type whereby dating and casual sexual relationships tended to elicit public dissemination of intimate images whilst domestic relationships and marriages (spousal separation) tended to elicit public dissemination to corporate web pages and to the victim's friends and/or family. These *tracks* for offending within the respective scenes/stages of the crime scripts are valuable in helping us distinguish between dating, domestic and sexual abuse within adult RS-IBSA, and to propose potential intervention points.

The three crime scripts helped us understand the rational decisions made by adult RS-IBSA offenders at each stage of the crime-commission process. In this vein, we propose several crime intervention points (Table 2) to increase offender handling, capable guardianship and place management with the purpose of disrupting and preventing RS-IBSA using Clarke and Eck's (2003) crime triangle (Fig. 5), which illustrates that three elements (offender, place and victim) must converge for RS-IBSA offending to occur. Ensuring the presence of capable guardians and place managers are likely to reduce criminal opportunities (Felson 2008).

At the *offender-victim prehistory stage*, there could be more education and awareness initiatives in areas of: (1) healthy relationship building and management; (2) understanding the realities of intimate relationships (e.g., relationships can fail); (3) post-relationship self-management; (4) signs of intimate partner abuse; (5) online and offline consent and privacy in different relationship contexts; (6) engaging in communication and negotiation of personal boundaries; (7) harms perpetuated and amplified by the Internet for adult RS-IBSA victims; (8) negative consequences for adult RS-IBSA offending (e.g., criminal conviction); (9) promoting safe and effective bystander intervention; and (10) increased institutional and police support for whistle-blowers (increasing presence of capable guardianship).

In the *crime set-up phase* (setting and instrumental actualisation stages), as place managers, online platforms can increase their technical controls for RS-IBSA offending and enhance their security and privacy features/settings for potential targets to utilise whilst intermediaries

Table 2 Adult RS-IBSA crime intervention points

Script stages	Manager-place	Guardian-target	Handler-offender
1. Offender- victim and prehistory		Establish clear boundaries General education regarding IBSA and potentially risky circumstances (i.e., reputational damage, psychological and physical harm) Partners Understanding both partners' attitudes and perceptions about IBSA will bring more awareness in the event of any 'triggers' (e.g., break-ups, fights, saying "No"), online and physical privacy and respect for consent Be aware that changes in the relationship (e.g., rejection, break-ups) may influence partners' actions and potentially alter dynamics and safety around them Be aware that gateway offences to IBSA (e.g., intimate covert filming and blackmail) are more latent Be aware that offending does not always occur immediately after a break-up Be aware that repeat victimisation and offending occurs more easily on the internet (i.e., images disclosed on the internet could resurface in future)	Public awareness of IBSA (issues around online and offline privacy, consent, intentional non-consent and potential contexts: e.g., break-ups, refusal to get back together, infidelity, new partner) (Barmore 2015; Gissell 2015; Salter and Crofts 2015) Partners Pre-establish boundaries, discuss boundaries, discuss concepts regarding IBSA perceptions, definitions, acceptable and non-acceptable behaviours, possible scenarios relating to consent and respect for online and offline privacy (Dawkins 2015)
2. Setting offline and online	Social media sites testing tools to help people manage how they interact with former partners on social media after a relationship Online platforms and intermediaries specialising in providing practical support to IBSA victims Online platforms increasing technical controls against potential IBSA	Monitor offline and cyberstalking behaviours, verbal abuse on social media Check on female (e.g., "How is ex responding to new male friend?"), signs of blackmail (e.g., abuser demanding sexual favours in exchange of non-disclosure) and other coercive control techniques (e.g., cutting off social support or financial support for child) If socio-cultural minority, check for signs of blackmail, verbal threats (e.g., threats to "out" victim or inform victim that law enforcement/ intermediaries would not help them due to their socio-cultural orientation)	Presence of friends/family can act as handlers Law enforcement's online and offline presence and efforts against IBSA
3. Instrumental actualisation	Have guardians present in location/at risk sites (social media) and moderators to maintain a strong and continued online presence Prompts to log out of social media when not in use	If in direct contact with abuser, do not provide positive reinforcement and discourage IBSA Alert victim immediately of the risk If there is a high risk of disclosure, support victim to contact intermediary for additional advice and practical support for "potential" takedown requests and future actions. If aware of the content of the images and the platforms that will be used in the disclosure, support the victim in reporting this possibility to the respective platforms	Increase public awareness in terms of guardianship and the role and practices required by encouraging people to actively look out for each other and identify circumstances in which men and women may be vulnerable

Table 2 (continued)

Script stages	Manager-place	Guardian-target	Handler-offender
4. Offender approach method	Having general security and privacy settings in place Having reporting and flagging of images protocols in place Information Service Providers (ISPs) and Social Media organisations should recalibrate anonymity standards to deter "anonymous" IBSA using the same tools and collaborative techniques they are utilising to fight terrorism	Education regarding common coercive control strategies (e.g., blackmail and threats) and ways to respond safely and effectively Education and encouragement against peer pressure and to develop resilience Education on online and physical safety—fully utilising general security and privacy settings on mobile devices and mobile apps to protect against physical level threats (Imgraben et al. 2014) (e.g., two-step authentication to access phone, logging out of social media apps and e-mail accounts when not in use, storing intimate images in "hard-to-reach" folders that are encrypted with strong passwords, not disclosing passwords to partners, disabling automatic password saving functions and location settings, not allowing anyone to physically handle or use your mobile device without your supervision, if you have intimate images, never capture identifying features/backgrounds- face, tattoos etc.) being careful to delete all intimate images (including Cloud back-ups) when sending phones for repair, trading-ins or disposing of them How to report and flag images	Remove excuses- general education on severe "privacy" and "trust" violations in relation to intimate partner violence and IBSA (e.g., "not knowing it is abuse" or "just for fun") (Albury and Crawford 2012; Powell 2010; Salter and Crofts 2015) International legal harmonisation (e.g., the criminalising of IBSA and EU's 'The Right to Be Forgotten') Intermediaries maintaining close ties with online platforms Law enforcement alerting public that there are convictions and incarcerations for IBSA
5. Continuation	Domestic intermediaries' and information service providers' ability to take immediate action on takedown requests and combat IBSA	Support victim in maintaining a positive online presence	Remove excuses-widespread messages against intimate partner violence and family violence and offences through digital communications technologies IBSA is committed by those who have complete disregard for consent and online and offline privacy IBSA is a domestic (sexual) violence offence and a communications offence (Bloom 2014) Alerting the public to the potential criminal consequences of doxing (online disclosure of a victim's personal details such as the victim's full name, e-mail address, residential address, designation and place of employment or mobile number) multiplies risk to a victim's personal and online safety (i.e., possible identity theft, in-the-flesh and online stalking and harassment)

Table 2 (continued)

Script stages	Manager-place	Guardian-target	Handler-offender
6. Interaction and crime completion	Online platforms to regularly prompt users to maximise use of security and privacy settings Have effective avenues for IBSA victims to report their victimisation and flag new intimate images that surface or resurface	Support victim with personal online safety strategies (e.g., disable settings for location and friends tagging you in photos and checking you into places, control visibility) Support victim with information on how to flag and report images	
7. Post-action	Assist intermediaries and law enforcement with criminal investigations	Do not download, consume for personal pleasure or distribute intimate images of victim Do not inform anyone else where to find the images and the contents of the images If others have encountered and threaten to circulate the victim's images, inform them that they might be interfering with police investigations and risk incriminating themselves in the process Support victim with creating a digital evidence folder (documenting dates for online disclosure and victim finding out, URLs, screen names and usernames, taking screenshots and downloading copies of images from website, reporting abuse to the online platforms and flagging abusive content) Supporting the victim with monitoring new content through Google reverse image searches for image file names, victim's phone number, name or other words or usernames associated with victim's images Supporting victim with setting up a Google Alert to notify victim of new content about victim that needs to be removed	Education regarding victim blaming, slut shaming by law enforcement and intermediaries: Sexting is a safety issue and not a moral issue (Slane 2013)
8. Exit	Keep digital evidence intact Monitor repeat offending on same account or new accounts with similar image-based abusive patterns	Encourage victim not to delete personal social media account (doing so would make it harder to push negative content off top search pages of internet search engines) Assist victim with creating new positive content on highly indexed pages Establishing emotional support hotlines for victims Education for friends and family regarding victim support Encourage reporting Continue to support victim in maintaining a positive online presence	

Fig. 5 The crime triangle [Adapted from "Fig. 1. The crime triangle (adapted from Clarke and Eck 2003)" in Cockbain and Laycock (2017)]

(if present) can increase their level of support for RS-IBSA victims. The police can also adequately support the intermediary by intervening in cases where offenders are non-compliant and persistent in their offending. Additionally, social media platforms can constantly prompt users to log out of their accounts when not in use. Increased public awareness of the harms inflicted by offenders on RS-IBSA victims and support for more aggressive RS-IBSA prevention efforts would improve the presence of capable guardianship (i.e., friends and family of the target including third parties). Capable guardians may then be less likely to resort to harm minimisation and victim blaming attitudes and would be more efficient and effective in supporting a potential RS-IBSA victim. Capable guardians can also be present in at-risk online platforms and maintain a strong online presence to deter offenders. Additionally, the police can also more actively utilise digital and print media to deter potential offenders.

During the *offender approach stage*, smartphone, online platforms and information service providers could strengthen their general and security privacy settings to bolster against personal online risk and physical-level security threats. These should be user-friendly and include compulsory security features to reduce the risk of victimisation (e.g., mandatory two-step authentication and logging out of social media and e-mail accounts). Smartphone providers can also enhance their intimate image protection systems by prompting users to delete, securely store and exclude self-taken intimate images from cloud back-ups. Smartphone providers can also use algorithms to alert users that their self-taken intimate images capturing identifying features will be deleted and outstanding intimate images would be wiped out from their smartphone in addition to the recipient's smartphone according to the terms of the sender. Education initiatives on how third parties can detect commonly used coercive control strategies in RS-IBSA (e.g., blackmail and threats), building resilience against participating in the circulation of a victim's images and supporting potential victims with personal security and the process of reporting their victimisation could also improve capable guardianship and deter RS-IBSA offenders. The police and/or relevant public sector agencies and charities also have a role in removing excuses for potential RS-IBSA offenders such as alerting the public to the risk of incarceration; that offenders are not entitled to leniency by the law even while offending under the influence of alcohol and/or drugs; and the irrelevance of whether the victim consented to share the intimate images with the offender and/or be photographed/filmed (victim blaming in any form is unacceptable).

At the *continuation* and *interaction and crime completion stages*, the crime intervention points involve targeted support for adult RS-IBSA victims from intermediaries and online platforms in ensuring immediate takedowns and takedown success. Capable guardians can also support an RS-IBSA victim in maintaining a positive online presence in the unfortunate circumstance that the intimate images are circulated widely on the Internet. The criminal justice system also has a significant role to play in leading and supporting initiatives against dating violence, technology-facilitated domestic and sexual violence and reducing harm minimisation and victim blaming attitudes in the public. Effective legislation of RS-IBSA as a communications offence and domestic and/or sexual abuse offence would improve support for victims seeking fair access to criminal justice. This would ensure that police resources are channelled adequately towards supporting adult RS-IBSA victims through reporting and where necessary, the entire investigative process. Adult RS-IBSA victims would benefit greatly from safe and immediate police intervention. Streamlining adult RS-IBSA victim support information would assist with protecting victims from further harm and possibly re-victimisation. Adequate support of adult RS-IBSA victims could also deter potential offenders. In addition, the police could also increase their investigative efforts into IBSA offences involving doxing which expose an RS-IBSA victim to further harm and risk of physical stalking, sexual harassment and sexual assault. Online platforms could continue to remind users to maximise use of their privacy/security settings and encourage online safety.

In the *post-action* and *exit stages*, the collaboration between intermediaries, online platforms and law enforcement must be robust. Guardians play a significant role in situational prevention by not circulating, storing

or consuming the non-consensually disseminated intimate images or inadvertently contributing to further dissemination by third parties. Capable guardians are also able to support the victim through reporting, filing takedown requests, maintaining a digital evidence folder in the event that their IBSA victimisation requires criminal investigation, counteracting the indexing on search engines and directing the victim to emotional support hotlines or mental health services if serious emotional distress was suffered. Finally, more effort must be targeted at minimising victim blaming.

A few limitations exist in this study. The use of court data may be susceptible to inaccuracies due to incorrect recording, lack of details or a prioritisation of certain aspects of a crime (Porter 2008). For instance, it was difficult to find reliable trends for RS-IBSA offending as some court transcripts were more detailed in documenting offending patterns than others. We could not investigate offender-victim prehistories which did not evidence abuse due to the omission of this information in the court transcripts. Future research could utilise police case files and offender and victim interviews to address the gaps in RS-IBSA offending literature. Utilising alternative data sources in addition to court records will enable us to represent adult RS-IBSA in an overall draft crime script (see Chiu and Leclerc 2017) and improve the proposed crime intervention points. Secondly, due to a lack of quantitative secondary data (court records and other sources) on all the types of RS-IBSA offending, this study is not representative of all RS-IBSA cases nationally, internationally or globally. Thirdly, we only documented one instance of RS-IBA in a casual sexual relationship which started online and transitioned into the offline space. Due to the inadequate data on this particular relationship dynamic and circumstances, we are unable to thoroughly investigate and propose protective strategies for RS-IBSA victims whose relationships started in the online space. However, with more reporting and recording, future research can operationalise a wider repertoire of RS-IBSA script tracks and acts in various intimate relationship types. Collectively, these would assist in revising and refining the three RS-IBSA crime scripts and proposed crime intervention points at every crime script stage.

We hope that developing crime scripts for RS-IBSA supports law enforcement agencies in their efforts to surmount possible jurisdictional and resourcing barriers around responding to RS-IBSA offenders in a timely and effective manner and ensuring community safety. Overall, this research has demonstrated that the greatest potential impact is in controlling and disrupting dating/domestic/marital spousal/sexual abuse in the offline space before it transitions into RS-IBSA in the online space, where there is potential for the harms to be immediate, and widespread and prolonged. More specifically, the crime scripts we devised have utility in helping law enforcement agencies and policy makers understand the crime-commission process of adult RS-IBSA and the various *tracks*, resources and locations involved in the offending.

The crime intervention points we propose in this study serve as building blocks for situational prevention efforts in future. Although this study identified important crime intervention points for the police (handlers) in offline spaces, we also acknowledge the impact of other controllers such as place managers and capable guardians in disrupting RS-IBSA in online spaces. This is an important research area that warrants further investigation. More specifically, future research could continue to expand the evidence base for RS-IBSA through crime scripts and investigate the role of controllers in situational prevention. For instance, more effective safeguarding of online spaces by handlers and controllers may be better addressed using the 25-techniques for situational prevention (Cornish and Clarke 2003). The specificity, structured and systematic nature of this framework would better equip policy makers and law enforcement agencies with disrupting the crime-commission process of RS-IBSA which occurs in offline and online spaces.

We also emphasise the need for law enforcement agencies' presence in safeguarding online spaces especially in instances where there is breach of police protection orders, persistent offending, and concealing the origins of the intimate images. We propose that law enforcement agencies focus on the crime script stage *offender-victim prehistory,* which we outline as a critical component of effective crime prevention strategies in view of the crime intervention points we have identified in this stage. During the *crime set-up phase*, we have identified more areas for situational prevention, specifically in the areas of enhancing physical-level personal security. We propose that law enforcement agencies participate more actively in disrupting the offender's *crime set-up phase* before the offender transitions into the *crime-achievement phase,* which takes place in the online space. From a policing perspective, it is more difficult to control and disrupt RS-IBSA once the offender initiates the deployment of online spaces and digital strategies.

Concluding remarks

We acknowledge that situational prevention is challenging given that the adult RS-IBSA offender-victim prehistory crime script stage may or may not evidence prior abuse, given the hidden nature of dating/domestic/sexual crimes. In this regard, future research could focus

on tailoring prevention strategies to specific circumstances and offender-victim relationships in addition to building standardised situational prevention strategies once sufficient crime scripting has been conducted on a larger sample of RS-IBSA offenders. This would ensure that offender handlers (law enforcement agencies), place managers (communications device corporations/websites, mobile application administrators/social media administrators and moderators) and capable guardians (third parties) are in the right online/offline spaces at the right times to prevent RS-IBSA offending.

By deconstructing adult RS-IBSA in the form of crime scripts and identifying crime prevention points at each crime script stage, we have helped distinguish between early stage and late stage situational prevention strategies throughout the entire crime-commission process of RS-IBSA. In addition, we propose that law enforcement agencies utilise the crime scripts and crime intervention points to guide adult RS-IBSA investigation, response and victim support processes. Lastly, we hope that more research can be conducted on RS-IBSA offender decision-making and offending behaviour in non-apprehended offenders. We acknowledge that this research only documents prosecutions. Emphatically, accounting for all RS-IBSA cases is a crucial step in preventing further displacement of dating/domestic/sexual abuse (and violence) into online/digital spaces.

Competing interests
The authors declare that they have no competing interests.

Authors' contributions
ACO collected the data, performed the data analysis and drafted the manuscript under the guidance of Prof. LM. Revisions were made by Prof. RKLK and Dr JRR. All authors read and approved the final manuscript.

Author details
[1] School of Social Science, The University of Queensland, Brisbane, QLD 4072, Australia. [2] School of Information Technology and Electrical Engineering, The University of Queensland, Brisbane, QLD 4072, Australia.

Appendices

Appendix 1

Offender profiles (n = 18)

Offender/case number	Case citation
1[b]	CRI-2016-042-000075 [2016] NZDC 6749
2	CRI-206-025-000506 [2016] NZDC 12912
3	CRI-2016-019-001079 [2016] NZDC 16010
4	CRI-2016-009-005981 [2016] NZDC 22470
5	CRI-2015-044-004701 [2017] NZDC 4615
6	CRI-2015-092-010077 CRI-2015-092-013167 [2016] NZDC 23957
7	CRI-2016-090-00217 [2017] NZDC 8269
8	CRI-2016-035-000873 [2017] NZDC 10417
9	CRI-2016-092-008720 [2017] NZDC 16230
10	CRI-2017-012-000185 [2017] NZDC 17182
11	CRI-2016-006-000610 [2017] NZDC 20663
12	CRI-2017-090-002585 [2017] NZDC 26347
13[b]	CRI-2017-018-000229 [2017] NZDC 24814
14[a]	CRI-2016-087-000921 [2016] NZDC 18572 CRI-2017-087-000516 [2017] NZDC 22077
15	CRI-2017-044-003427 [2017] NZDC 28981
16[b]	CRI-2017-011-000157 [2018] NZDC 2910
17	CRI-2017-091-001700 [2018] NZDC 6846
18	CRI-2017-012-001974 [2018] NZDC 16646

[a] Offender Profile/Case Number 14 has two different court hearings

[b] For Case Number 1, 13 and 16, the complainants/victims in the court hearings were the recipients of non-consensually disseminated intimate images (i.e., a mother, 16-year old son, and daughter respectively). In this study, we label victim as the individual whose intimate images were disseminatedAppendix 2

See Table 3.

Table 3 Data categorisation from court transcripts (Chiu and Leclerc 2017, p. 64–65)

Variables	Categories
Social elements	
Actors involved	Offender, victim, co-offenders, third parties (victim's children; partners; other relatives and other known--- friends, acquaintances, co-workers, housemates)
Relationship between victim and offender	Date, partner or ex-partner (including husband, boyfriend, de facto partner, and sex friend), relative, friend/acquaintance, co-worker or ex co-worker, neighbour, family member's spouse
Circumstances	Date rape, break in, group outing, visitation
Approach method	
Con	Offered or asked for assistance/ride/information, etc. Solicitation for sex Wanted to show something to victim Bribed victim with money, drugs, etc.
Surprise	Victim was asleep Lay in wait/snuck up on victim
Blitz	Used weapon Used overwhelming force or violence
Setting	
Location	Offender's home, victim's home, vehicle, other residence, other building, outdoors
More than one crime scene	Yes/no
Time	Daylight, darkness
Interaction	
Victim reaction	Forceful verbal resistance (screamed, yelled/yelled for help), non-forceful verbal resistance (said no, pleaded, used threats), cried, physical resistance (fought back, tried to escape), no victim reaction, compliance, called police, negotiation
Offender reaction	Ignored, used force, used threats, used violence, negotiated, ceased to demand
Sexual acts	Kissing, grabbing/hugging, fondling, digital penetration, vaginal penetration, anal penetration, cunnilingus, fellatio, masturbation, suffocation, choking, beating/slapping
Other variables	
Disruption	Third party intervened/disrupted, victim escaped
Exit	Offender left scene, victim left scene, offender dropped victim home, victim dropped offender home, victim passed out
Threats/force	Threats used, violence used, weapon used
Tools/transport	Weapon, car, condom, gag, bindings, disguise, other (e.g., alcohol, victim's keys, removed car door handle)
Post-action	Apologies, threats, tried to comfort/be intimate with victim, tried to ask victim on a date, told victim not to tell anyone, stole from victim, told victim not to move
Variables	Categories
Other	Potential 'triggers' (date/sexual advance rejection, prior relationship break-up), prior alcohol consumption (victim, offender), prior drug consumption, offender removed clothing, offender made victim remove clothing, moderate-to-severe victim injury, alcohol consumed during offence, drugs involved during offence

The term 'trigger' refers to factors or offender-victim prehistory that may result in the offender being in a heightened emotional state (e.g., stress/anger), and is not intended to imply causality

Appendix 3

See Fig. 6.

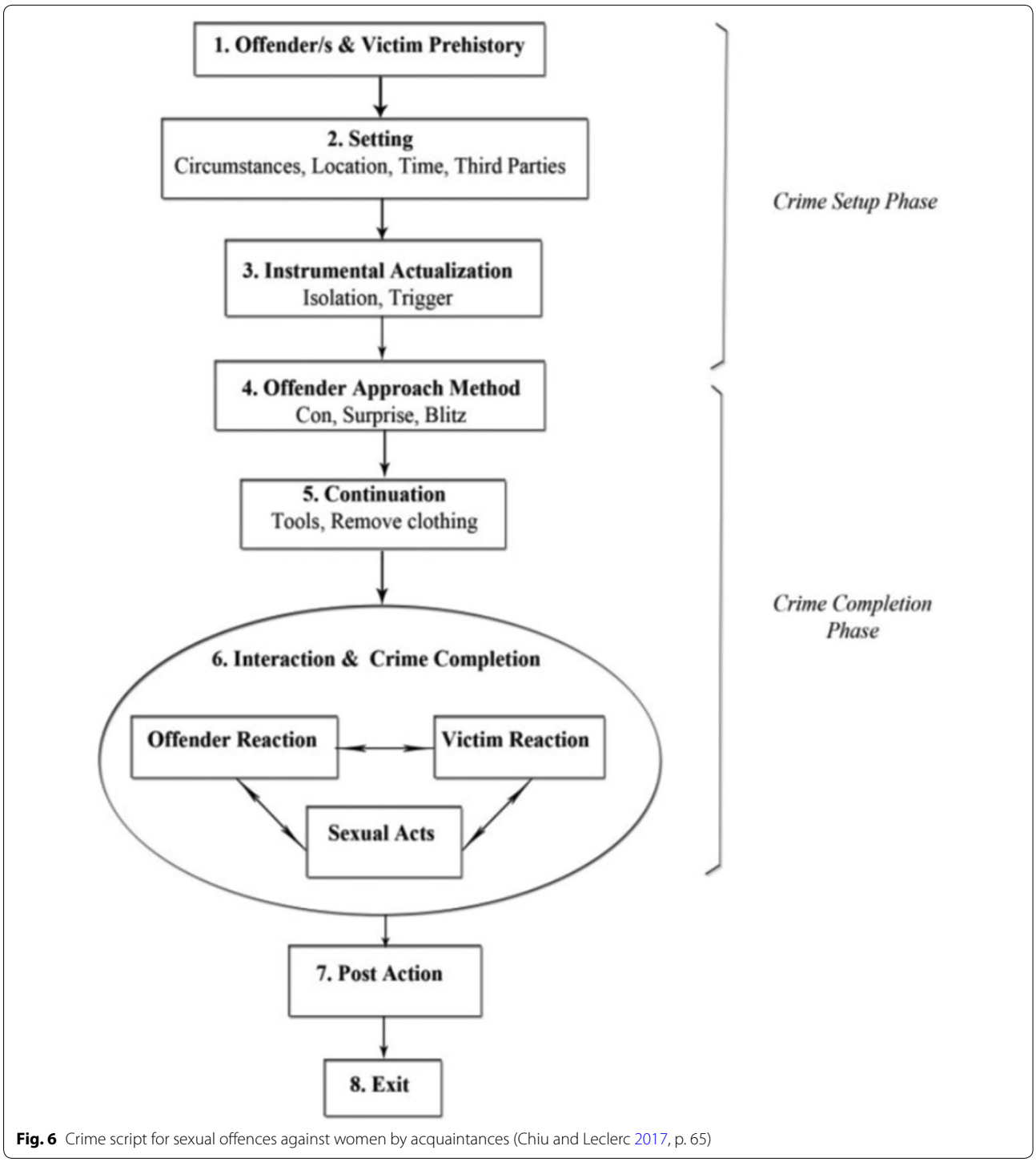

Fig. 6 Crime script for sexual offences against women by acquaintances (Chiu and Leclerc 2017, p. 65)

Appendix 4

See Fig. 7.

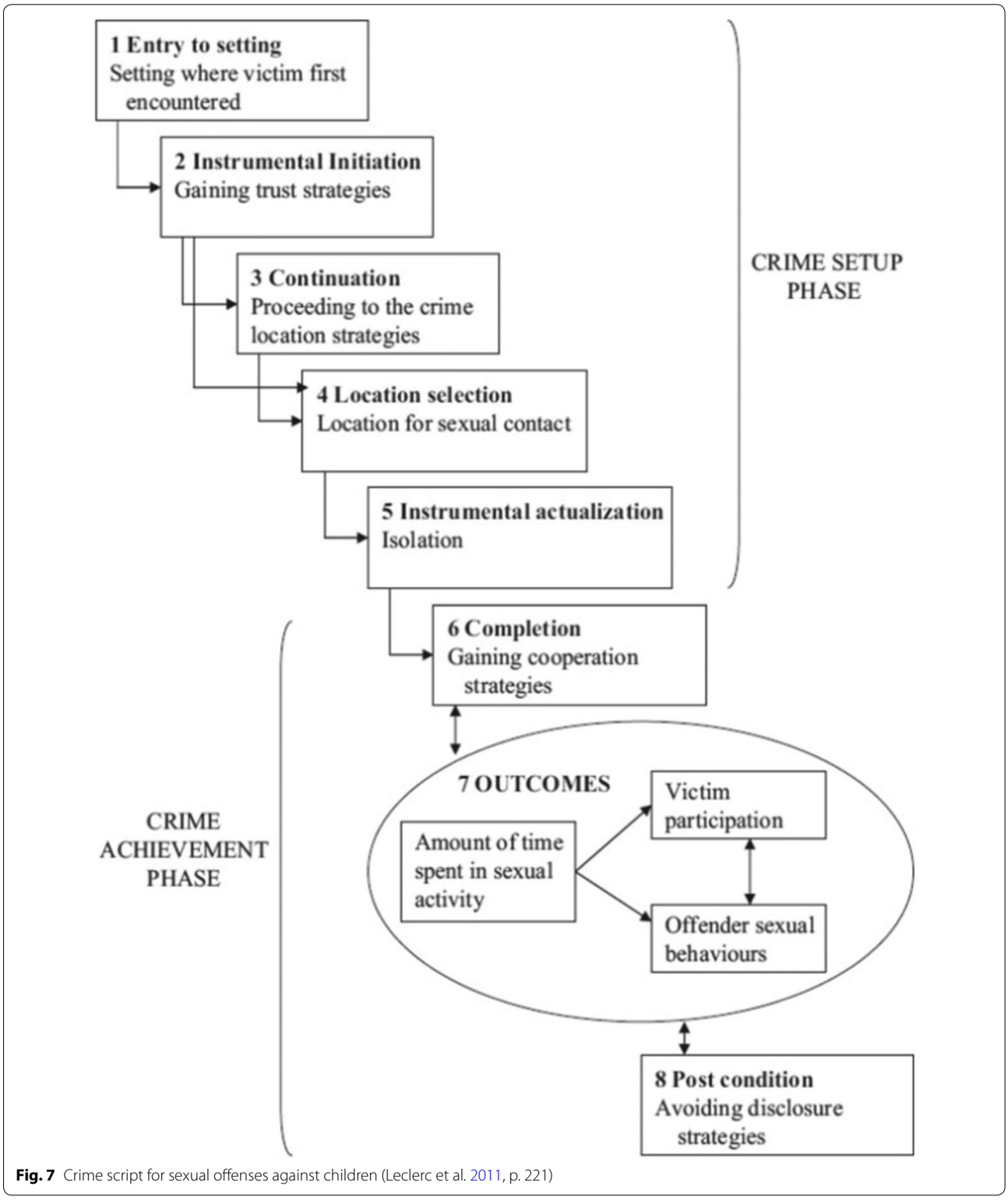

Fig. 7 Crime script for sexual offenses against children (Leclerc et al. 2011, p. 221)

Received: 11 July 2020 Accepted: 9 October 2020
Published online: 02 December 2020

References

Abelson, R. P. (1976). Script processing in attitude formation and decision making. In J. S. Carroll & J. W. Payne (Eds.), *Cognition and social behavior*. New Jersey: Lawrence Erlbaum.

Abelson, R. P. (1981). Psychological status of the script concept. *American Psychologist, 36*(7), 715–729. https://doi.org/10.1037/0003-066X.36.7.715.

Albury, K., & Crawford, K. (2012). Sexting, consent and young people's ethics: Beyond Megan's Story. *Continuum, 26*(3), 463–473. https://doi.org/10.1080/10304312.2012.665840.

Balemba, S., & Beauregard, E. (2013). Where and when? Examining spatiotemporal aspects of sexual assault events. *Journal of Sexual Aggression, 19*(2), 171–190. https://doi.org/10.1080/13552600.2012.703702.

Barmore, C. (2015). Criminalization in context: Involuntariness, obscenity, and the First Amendment. *Stanford Law Review, 67*(2), 447–478.

Bates, S. (2017). Revenge porn and mental health: A qualitative analysis of the mental health effects of revenge porn on female survivors. *Feminist Criminology, 12*(1), 22–42. https://doi.org/10.1177/1557085116654565.

Baym, N. (2015). Social media and the struggle for society. *Social Media Society*. https://doi.org/10.1177/2056305115580477.

Beauregard, E., & Martineau, M. (2015). An application of CRAVED to the choice of victim in sexual homicide: A routine activity approach. *Crime Science, 4*(24), 1–11. https://doi.org/10.1186/s40163-015-0036-3.

Beauregard, E., Proulx, J., Rossmo, K., Leclerc, B., & Allaire, J.-F. (2007). Script analysis of the hunting process of serial sex offenders. *Criminal Justice and Behavior, 34*(8), 1069–1084. https://doi.org/10.1177/0093854807300851.

Bichler, G., Bush, S., & Malm, A. (2013). Bad actors and faulty props: Unlocking legal and illicit art trade. *Global Crime, 14,* 359–385. https://doi.org/10.1080/17440572.2013.828999.

Bloom, S. (2014). No vengeance for 'revenge porn' victims: Unraveling why this latest female-centric, intimate-partner offense is still legal, and why we should criminalize it. *Fordham Urban Law Journal, 42,* 233–289.

Bluett-Boyd, N., Fileborn, B., Quadara, A., & Moore, A. D. (2013). The role of emerging communication technologies in experiences of sexual violence: A new legal frontier? *Journal of the Home Economics Institute of Australia, 20*(2), 25.

Borrion, H. (2013). Quality assurance in crime scripting. *Crime Science, 2,* 6. https://doi.org/10.1186/2193-7680-2-6.

Brantingham, P. L., & Brantingham, P. J. (1978). A topological technique for regionalization. *Environment and Behavior, 10*(3), 335–353. https://doi.org/10.1177/0013916578103004.

Brayley, H., Cockbain, E., & Laycock, G. (2011). The Value of Crime Scripting: Deconstructing Internal Child Sex Trafficking. *Policing: A Journal of Policy and Practice, 5*(2), 132–143. https://doi.org/10.1093/police/par024.

Chiu, Y. N., & Leclerc, B. (2017). An examination of sexual offenses against women by acquaintances: The utility of a script framework for prevention purposes. In *Crime Prevention in the 21st Century: Insightful Approaches for Crime Prevention Initiatives* (pp. 59–76). Springer International Publishing, Berlin.

Chiu, Y., Leclerc, B., & Townsley, M. (2011). Crime Script Analysis of Drug Manufacturing In Clandestine Laboratories: Implications for Prevention. *British Journal of Criminology, 51*(2), 355–374. https://doi.org/10.1093/bjc/azr005.

Clarke, R. V. G., & Cornish, D. B. (1983). *Crime control in Britain: A review of policy research*. Albany: SUNY Press.

Clarke, R. V., & Cornish, D. B. (1985). Modeling offenders' decisions: A framework for research and policy. *Crime and Justice, 6,* 147–185. https://doi.org/10.1086/449106.

Clarke, R. V. & Eck., J. (2003). *Become a Problem Solving Crime Analyst.* Jill Dando Institute of Crime Science, Devon. https://popcenter.asu.edu/sites/default/files/library/reading/PDFs/55stepsUK.pdf.

Cockbain, E., & Laycock, G. (2017). Crime science. In H. N. Pontell (Ed.), *Oxford research encyclopedia of criminology and criminal justice* (pp. 1–37). Oxford: Oxford University Press. https://doi.org/10.1093/acrefore/9780190264079.013.4.

Cook, D. (1997). *Poverty, crime and punishment* (p. 127). London: CPAG.

Cook, A., Reynald, D. M., Leclerc, B., & Wortley, R. (2019). learning about situational crime prevention from offenders: Using a script framework to compare the commission of completed and disrupted sexual offenses. *Criminal Justice Review, 44*(4), 431–451. https://doi.org/10.1177/0734016818812149.

Cornish, D. B. (1994a). The procedural analysis of offending and its relevance for situational prevention. In R. V. Clarke (Ed.), *Crime prevention studies* (vol. 3, pp. 151–196). Monsey, NY: Criminal Justice Press.

Cornish, D. B. (1994b). Crime as scripts. In D. Zahm, & P. Comwell (Eds.), *Proceedings of the International Seminar on Environmental Criminology and Crime Analysis* (Volume 1, pp. 30–45). Tallahassee, FL: Florida Statistical Analysis Center, Florida Criminal Justice Executive Institute, Florida Department of Law Enforcement.

Cornish, D. B., & Clarke, R. V. G. (1986). *The reasoning criminal: Rational choice perspectives on offending*. Berlin: Springer.

Cornish, D. B., & Clarke, R. V. (1987). Understanding crime displacement: An application of rational choice theory. *Criminology, 25*(4), 933–947. https://doi.org/10.1111/j.1745-9125.1987.tb00826.x.

Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal dispositions: A reply to Wortley's critique of situational crime prevention. *Crime Prevention Studies, 16,* 41–96.

Cornish, D. B., & Clarke, R. V. (2006). The rational choice perspective. In S. Henry & M. M. Lanier (Eds.), *The essential criminology reader* (pp. 18–29). Boulder: Westview Press.

Cornish, D. B., & Clarke, R. V. (2008). The rational choice perspective. In R. Wortley & L. Mazerolle (Eds.), *Environmental criminology and crime analysis* (pp. 29–47). Cullompton: Willan.

Crossman, K. A., Hardesty, J. L., & Raffaelli, M. (2016). "He could scare me without laying a hand on me": mothers' experiences of nonviolent coercive control during marriage and after separation. *Violence Against Women, 22*(4), 454–473. https://doi.org/10.1177/1077801215604744.

Cusson, M. (1983). *Why delinquency?*. Toronto: University of Toronto Press.

Dawkins, J. T. (2015). A dish served cold: The case for criminalizing revenge pornography. *Cumberland Law Review, 45,* 395–447.

de Vries, M. S. (2013). From the instrument of delivery to the actual agent of harm: Fighting the criminal purchase of ammunition. *European Journal on Criminal Policy and Research, 19*(1), 1–14. https://doi.org/10.1007/s10610-012-9173-3.

Dehghanniri, H., & Borrion, H. (2019). Crime scripting: A systematic review. *European Journal of Criminology*. https://doi.org/10.1177/1477370819850943.

DeKeseredy, W. S., & Schwartz, M. D. (2016). Thinking sociologically about image-based sexual abuse: The contribution of male peer support theory. *Sexualization, Media, & Society.*,. https://doi.org/10.1177/2374623816684692.

Deslauriers-Varin, N., & Beauregard, E. (2010). Victims' routine activities and sex offenders' target selection scripts: A latent class analysis. *Sexual Abuse, 22*(3), 315–342. https://doi.org/10.1177/1079063210375975.

Douglas, D. M. (2016). Doxing: A conceptual analysis. *Ethics and Information Technology, 18*(3), 199–210. https://doi.org/10.1007/s10676-016-9406-0.

Dragiewicz, M., Burgess, J., Matamoros-Fernández, A., Salter, M., Suzor, N., Woodlock, D., et al. (2018). Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms. *Feminist Media Studies, 18*(4), 609–625. https://doi.org/10.1080/14680777.2018.1447341.

Draucker, C. B., & Martsolf, D. S. (2010). The role of electronic communication technology in adolescent dating violence. *Journal of Child and Adolescent Psychiatric Nursing, 23*(3), 133–142. https://doi.org/10.1111/j.1744-6171.2010.00235.x.

Drouin, M., Vogel, K. N., Surbey, A., & Stills, J. R. (2013). Let's talk about sexting, baby: Computer-mediated sexual behaviors among young adults. *Computers in Human Behavior, 29*(5), A25–A30. https://doi.org/10.1016/j.chb.2012.12.030.

Einstadter, W., & Henry, S. (2006). *Criminological theory: An analysis of its underlying assumptions* (2nd ed.). Lanham: Rowman & Littlefield.

Ekblom, P., & Gill, M. (2015). Rewriting the script: Cross-disciplinary exploration and conceptual consolidation of the procedural analysis of crime. *European Journal on Criminal Policy and Research, 22*(2), 319–339. https://doi.org/10.1007/s10610-015-9291-9.

Ekblom, P., & Sidebottom, A. (2008). What do you mean, 'Is it secure?' Redesigning language to be fit for the task of assessing the security of domestic

and personal electronic goods. *European Journal on Criminal Policy and Research, 14*(1), 61–87.
Felson, M. (2008). Routine activity approach. In R. Wortley & L. Mazerolle (Eds.), *Environmental criminology and crime analysis* (pp. 70–77). Devon: Willan Publishing.
Freilich, J. D., & Chermak, S. M. (2009). Preventing deadly encounters between law enforcement and American far-rightists. In J. D., Freilich, & G. R., Newman, (Eds.). *Reducing terrorism through situational crime prevention*. Crime Prevention Studies (Vol. 25, pp. 144–172). Boulder: Lynne Rienner Publishers.
Gissell, T. E. (2015). Felony count 1: Indecent disclosure. *Houston Law Review*, *53*, 273–301.
Grabosky, P. (2000). Cyber crime and information warfare. In *Proceedings of the Transnational Crime Conference.* (pp. 1–19). Canberra, 9–10 March. http://www.combattingcybercrime.org/files/virtual-library/phenomena-challenges-cybercrime/cyber-crime-and-information-warfare.pdf.
Haelterman, H. (2016). Crimes as scripts. *Crime script analysis: Preventing crimes against business* (pp. 7–26). London: Palgrave Macmillan. https://doi.org/10.1057/978-1-137-54613-5.
Hall, M., & Hearn, J. (2019). Revenge pornography and manhood acts: A discourse analysis of perpetrators' accounts. *Journal of Gender Studies, 28*(2), 158–170. https://doi.org/10.1080/09589236.2017.1417117.
Hatcher, M., McDannell, J., & Ostfeld, S. (1999). Computer crimes. *American Criminal Law Review, 36*(3), 397–444.
Hiller, J., & Cohen, R. (2002). *Internet law and policy*. Prentice Hall.
Imgraben, J., Engelbrecht, A., & Choo, K.-K. R. (2014). Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. *Behaviour & Information Technology, 33*(12), 1347–1360. https://doi.org/10.1080/0144929X.2014.934286.
Kelly, J. B., & Johnson, M. P. (2008). Differentiation among types of intimate partner violence: Research update and implications for interventions. *Family Court Review*, *46*(3), 476–499. https://doi.org/10.1111/j.1744-1617.2008.00215.x.
Langlois, G., & Slane, A. (2017). Economies of reputation: The case of revenge porn. *Communication and Critical/Cultural Studies, 14*(2), 120–138. https://doi.org/10.1080/14791420.2016.1273534.
Lavorgna, A. (2015). The online trade in counterfeit pharmaceuticals: New criminal opportunities, trends and challenges. *European Journal of Criminology, 12*(2), 226–241. https://doi.org/10.1177/1477370814554722.
Lavorgna. A. (2014). Transit crimes in the Internet age: How new online criminal opportunities affect the organization of offline transit crimes. Thesis, University of Trento, Italy.
Leclerc, B. (2013). New developments in script analysis for situational crime prevention: Moving beyond offender scripts. In B. Leclerc & R. Wortley (Eds.), *Cognition and crime: Offender decision-making and script analyses. Crime science series* (pp. 221–236). London: Routledge.
Leclerc, B., & Wortley, R. (Eds.). (2014a). *Cognition and crime. Offender decision making and script analyses* (p. 261). New York: Routledge.
Leclerc, B., & Wortley, R. (2014b). The reasoning criminal. Twenty-five years on. In B. Leclerc & R. Wortley (Eds.), *Cognition and crime. Offender decision making and script analyses* (pp. 1–11). New York: Routledge.
Leclerc, B., Wortley, R., & Smallbone, S. (2010). Investigating mobility patterns for repetitive sexual contact in adult child sex offending. *Journal of Criminal Justice, 38,* 648–656. https://doi.org/10.1016/j.jcrimjus.2010.04.038.
Leclerc, B., Wortley, R., & Smallbone, S. (2011). Getting into the script of adult child sex offenders and mapping out situational prevention measures. *Journal of Research in Crime and Delinquency, 48,* 209–237. https://doi.org/10.1177/0022427810391540.
Leddo, J., & Abelson, R. P. (1986). The nature of explanations. In J. A. Galambos, R. P. Abelson, & J. B. Black (Eds.), *Knowledge structures* (pp. 103–122). New Jersey: Lawrence Erlbaum Associates.
Li, X. (2014). Phenomenal exploration into impact of anonymity on law and order in cyberspace. *Kriminologija i Socijalna Integracija, 22,* 102–123.
Li, J. C. M. (2015). Adolescent compensated dating in Hong Kong: Choice, script, and dynamics. *International Journal of Offender Therapy and Comparative Criminology, 59*(6), 588–610. https://doi.org/10.1177/0306624X13516285.
Lord, N., & Levi, M. (2017). Organizing the finances for and the finances from transnational corporate bribery. *European Journal of Criminology, 14*(3), 365–389. https://doi.org/10.1177/1477370816661740.
McGlynn, C., Rackley, E., & Houghton, R. (2017). Beyond 'Revenge Porn': The continuum of image-based sexual abuse. *Feminist Legal Studies, 25,* 25–46. https://doi.org/10.1007/s10691-017-9343-2.
Melander, L. A. (2010). College students' perceptions of intimate partner cyber harassment. *Cyberpsychology, Behavior, and Social Networking, 13*(3), 263–268. https://doi.org/10.1089/cyber.2009.0221.
Meyer, S., Jore, S., & Werner Johansen, K. (2015). Troublesome trade-offs: Balancing urban activities and values when securing a city-centre governmental quarter. *City, Territory and Architecture.* https://doi.org/10.1186/s40410-015-0025-6.
Myhill, A. (2015). Measuring coercive control: What can we learn from national population surveys? *Violence Against Women, 21*(3), 355–375. https://doi.org/10.1177/1077801214568032.
Nee, C., & Meenaghan, A. (2006). Expert decision making in burglars. *British Journal of Criminology*. https://doi.org/10.1093/bjc/azl013.
Ornstein, P., & Rickne, J. (2013). When does intimate partner violence continue after separation? *Violence Against Women, 19*(5), 617–633. https://doi.org/10.1177/1077801213490560.
Pitman, T. (2017). Living with coercive control: Trapped within a complex web of double standards, double binds and boundary violations. *The British Journal of Social Work, 47*(1), 143–161. https://doi.org/10.1093/bjsw/bcw002.
Pittaro, M. (2007). Cyber stalking: An analysis of online harassment and intimidation. *International Journal of Cyber Criminology, 1*(2), 180–197. https://doi.org/10.5281/zenodo.18794.
Porter, L. E. (2008). Using archival data and multidimensional scaling to explore leadership: Examples from group crime. *Issues in Forensic Psychology, 8,* 33–44.
Powell, A. (2010). Configuring consent: EMERGING technologies, unauthorized sexual images and sexual assault. *Australian & New Zealand Journal of CRIMINOLOGY, 43*(1), 76–90. https://doi.org/10.1375/acri.43.1.76.
Powell, A., & Henry, N. (2017). Beyond 'Revenge Pornography'. In: *Sexual violence in a digital age*. Palgrave studies in cybercrime and cybersecurity. (pp. 117–152). London: Palgrave Macmillan. https://doi.org/10.1057/978-1-137-58047-4_5.
Powell, A., Henry, N., & Flynn, A. (2018). Image-based sexual abuse. In: W. S. Dekeseredy, & M. Dragiewicz (Eds.), *Routledge handbook of critical criminology* (2nd ed., pp. 305–315). Routledge, Abingdon.
Powell, A., Henry, N., Flynn, A., & Scott, A. J. (2019). Image-based sexual abuse: The extent, nature, and predictors of perpetration in a community sample of Australian residents. *Comput Hum Behav, 92,* 393–402. https://doi.org/10.1016/j.chb.2018.11.009.
Reed, L. A., Tolman, R. M., & Ward, L. M. (2016). Snooping and sexting: Digital media as a context for dating aggression and abuse among college students. *Violence Against Women, 22*(13), 1556–1576. https://doi.org/10.1177/1077801216630143.
Ruvalcaba, Y., & Eaton, A. A. (2020). Nonconsensual pornography among U.S. adults: A sexual scripts framework on victimization, perpetration, and health correlates for women and men. *Psychology of Violence, 10*(1), 68–78. https://doi.org/10.1037/vio0000233.
Salter, M., & Crofts, T. (2015). Responding to revenge porn: Challenges to online legal impunity. In L. Comella & S. Tarrant (Eds.), *New Views on Pornography: Sexuality, Politics, and the Law* (pp. 233–253). Goleta: Praeger.
Savona, E. U., Giommoni, L., & Mancuso, M. (2014). Human trafficking for sexual exploitation in Italy. In B. Leclerc & R. Wortley (Eds.), *Cognition and crime. Offender decision making and script analyses* (pp. 140–163). London: Routledge.
Schank, R., & Abelson, R. (1977). *Scripts, plans, goals, and understanding: An inquiry into human knowledge structures*. New Jersey: Lawrence Erlbaum Associates.
Slane, A. (2013). Sexting and the law in Canada. *The Canadian Journal of Human Sexuality, 22,* 117–122. https://doi.org/10.3138/cjhs.22.3.C01.
Somer, T., Tiido, A., Sample, C., & Mitchener-Nissen, T. (2018). Application of journey mapping and crime scripting to the phenomenon of trolling. In: *ICCWS 2018 13th International Conference on Cyber Warfare and Security* (p. 465). Academic Conferences and Publishing Limited.
Stroud, S. R. (2014). The dark side of the online self: A pragmatist critique of the growing plague of revenge porn. *Journal of Mass Media Ethics, 29*(3), 168–183. https://doi.org/10.1080/08900523.2014.917976.

Tompson, L., & Chainey, S. (2011). Profiling illegal waste activity: Using crime scripts as a data collection and analytical strategy. *European Journal on Criminal Policy and Research, 17,* 179–201. https://doi.org/10.1007/s10610-011-9146-y.
Tremblay, P., Talon, B., & Hurley, D. (2001). Body switching and related adaptations in the resale of stolen vehicles: Script elaborations and aggregate crime learning curves. *British Journal of Criminology*, *41*, 561–579.
Uhl, C. A., Rhyner, K. J., Terrance, C. A., & Lugo, N. R. (2018). An examination of nonconsensual pornography websites. *Feminism & Psychology, 28*(1), 50–68. https://doi.org/10.1177/0959353517720225.
Velonis, A. J. (2016). "He never did anything you typically think of as abuse": Experiences with violence in controlling and non-controlling relationships in a non-agency sample of women. *Violence Against Women, 22*(9), 1031–1054. https://doi.org/10.1177/1077801215618805.
Vitis, L. (2020). Private, hidden and obscured: Image-based sexual abuse in Singapore. *Asian Journal of Criminology, 15*(1), 25–43. https://doi.org/10.1007/s11417-019-09293-0.
Walsh, D. (1978). *Shoplifting: Controlling a major crime*. New York: Macmillan.
Willison, R., & Siponen, M. (2009). Overcoming the insider: Reducing employee computer crime through situational crime prevention. *Association for Computing Machinery Communications, 52*(9), 133–137. https://doi.org/10.1145/1562164.1562198.
Woodlock, D. (2017). The abuse of technology in domestic violence and stalking. *Violence Against Women, 23*(5), 584–602. https://doi.org/10.1177/1077801216646277.
Wortley, R. (2014). Rational choice and offender decision making. Lessons from the cognitive sciences. In: B. Leclerc & R. Wortley (Eds.), *Cognition and crime. Offender decision making and script analyses* (pp. 237–252). Routledge, Abingdon.
Wortley, R., & Mazerolle, L. (2013). Situating the theory, analytic approach and application. In R. Wortley & L. Mazerolle (Eds.), *Environmental criminology and crime analysis* (pp. 1–18). London: Willan Publishing.
Yar, M. (2005). The novelty of 'cybercrime' an assessment in light of routine activity. *European Journal of Criminology, 2,* 407–427. https://doi.org/10.1177/147737080556056.

Publisher's Note