Effects of automated messages on Internet users attempting to access 'barely legal' pornography

JEREMY PRICHARD [1] | RICHARD WORTLEY[2] | PAUL A. WATTERS[3] | CAROLINE SPIRANOVIC[1] | CHARLOTTE HUNN[1] | TONY KRONE[4]

[1]Law School, University of Tasmania–Australia

[2]Jill Dando Institute of Security and Crime Science, University College London–United Kingdom

[3]School of Engineering and Mathematical Sciences, La Trobe University–Australia

[4]Law School, University of Canberra–Australia

Correspondence

Jeremy Prichard, Law School, University of Tasmania, Australia.

Email: Jeremy.Prichard@utas.edu.au

Funding information

This project was funded by the Australian Government through the Australian Research Council (DP160100601).

KEYWORDS

child sexual exploitation material, situational crime prevention, pop-ups, warning banners, deterrence messages

Abstract

We examined whether online warning messages would dissuade individuals from visiting a honeypot website purporting to contain barely legal pornography. Participants (*n*=419) seeking the site were randomly assigned to one of five conditions; they went straight to the landing page (control; *n*=100), or encountered a warning message advising of the potential harm to viewers (*n*=74), potential harm to victims (*n*=65), ability of police to track IP addresses (*n*=81), or possible illegality of such pornography (*n*=99). Attrition rates for the warning message conditions were 38-52%, compared with 27% for the control group. The most effective messages were those that warned that IP addresses can be traced (OR=2.64) and that the pornography may be illegal (OR=2.99). Warning messages offer a valuable and cost effective strategy that can be scaled up to help reduce the accessing of child sexual exploitation material online.

INTRODUCTION

The scale of the market for child sexual exploitation material (CSEM[1]) now overwhelms police capacity. Increasingly, police are by necessity having to triage cases of CSEM offending, concentrating on the most serious offenders who are suspected of involvement in contact offending (Child Dignity Alliance, 2018; Seto, 2013). There is an urgent need to develop prevention strategies that can be rolled out with minimum resource commitment to help deal with less serious cases of CSEM viewing. Online warning messages have been recommended as one means to reduce the viewing of CSEM (Quayle & Kouropoulos, 2018; Williams, 2005; Wortley & Smallbone, 2012), especially by those who are in the early stages of an offending career (Taylor & Quayle, 2008). While a promising strategy, there is currently no evidence base for the efficacy of warning messages in this context. Moreover, disagreement exists as to whether such warnings should focus on deterrence or on the harms associated with CSEM production (Williams, 2005; cf Wortley & Smallbone, 2012). The present study responds to these knowledge gaps by examining whether different types of warning messages influence the behavior of Internet users at the moment they are attempting to view barely legal pornography – pornography that seeks to portray adult actresses as minors (Dines, 2009) – which we treat as a proxy for and possible gateway to CSEM.

The Case for Prevention

All available metrics indicate that CSEM is a major and growing problem (Internet Watch Foundation, 2017; Quayle et al., 2018; We Protect, 2019). In response, most jurisdictions now have specialised law enforcement agencies to tackle CSEM offending. However, the proportion of CSEM offenders arrested remains very small. In the UK, police

[1] We define CSEM broadly as including any material involving sexualized content of children (Prichard & Spiranovic, 2014).

estimates provided to a Parliamentary Committee indicated that approximately 5,400 people were arrested for CSEM offences each year in 2017 and 2018. The Committee estimated that only nine per cent of recorded incidents led to a charge (Home Affairs Committee, 2018, p. 38). With arrests in the thousands but the number of offenders estimated in the millions (We Protect, 2019), the need to diversify strategies beyond traditional law enforcement is obvious (Henzey, 2011). There are simply too many cases for law enforcement agencies to deal with, and this, coupled with the fact that offenders are more than likely to be outside the jurisdiction of the investigating agency, means that in the overwhelming majority of cases CSEM offenders will never be identified, much less caught. In the face of this reality, police need to concentrate their efforts on a relatively small core of the most serious offenders (Seto, 2013; for CSEM risk assessment tools to aid police in this task see Long, Alison, Tejeiro, et al., 2016; Seto & Eke, 2015).

Less resource-intensive prevention strategies may provide an effective alternative response for a significant proportion of CSEM offenders. There is evidence of different aetiological pathways into viewing CSEM (Merdian et al., 2018) and viewing may commence in the absence of a pedophilic disorder or a self-reported sexual interest in children (see for instance Ly et al., 2018). For these offenders, the process leading to developing a specific interest in CSEM may be gradual and eventually involve crossing a "significant psychological threshold" (Wortley & Smallbone, 2012, p.121). In other situations the first deliberate viewing of CSEM (onset) may be done "impulsively and/or out of curiosity" (Beech et al., 2008, p. 225; see also Lanning, 2010), although it seems likely that such a decision would be influenced by personal factors (e.g., sex drive, intoxication) and other factors (e.g., the absence of pro-social others, such as a spouse; see Seto, 2019). Critically, CSEM does not have to be deliberately sought. Opportunities to view CSEM are presented in various ways on the Internet, such as P2P networks (Prichard et al., 2011;

Prichard et al., 2013), email spam (Krone, 2004), website noticeboards (e.g., Rushkoff, 2009) and pop-up advertisements on adult pornography websites (Morgan & Lambie, 2019). Gateways into CSEM, as reported by CSEM users, include legal materials such as adult pornography, barely legal pornography, and child modelling sites (Morgan & Lambie, 2019). For individuals at risk of onset, early intervention may successfully divert them from viewing CSEM.

Situational crime prevention provides a useful framework for devising strategies to help reduce CSEM offending (Smallbone & Wortley, 2017; Wortley, 2012; Wortley & Smallbone, 2006a, 2012). The situational perspective posits that all crime is the result of a person-situation interaction, and that given the right circumstances even normally law-abiding individuals may offend (Clarke, 2017; Mayhew et al., 1975). The theoretical focus shifts from the offender's criminal disposition to environmental factors that permit or encourage the offence at a particular time and place. The Internet provides an ideal environment in which individuals with even a cursory sexual interest in minors can satisfy their curiosity (Wortley & Smallbone, 2006b; 2012). CSEM can be immediately accessed cheaply, with apparent anonymity and with low risk of detection, from the comfort of home (Merdian et al., 2009; Quayle, 2012; Wortley & Smallbone, 2006a, 2012). As Quayle (2012, p. 110) observes, there are few other crimes that an individual can commit with such "extraordinary ease." Situational CSEM-prevention strategies involve making the Internet a less conducive environment for offending (Smallbone & Wortley, 2017; Wortley, 2012; Wortley & Smallbone, 2006a, 2012). One promising situational strategy, discussed below, is the use of warning messages to influence the decision making of potential offenders at the very time they are seeking out CSEM.

Warning Messages

Scientific literature examining warning message compliance exists in areas such as public health, occupational safety, road safety, consumer protection, and crime prevention. Compliance has been found to increase when messages impart clear and concise information about hazards and the behavior needed to avoid them (Laughery & Smith, 2006; Lenorovitz, Leonard & Karnes, 2012); are believable (Riley, 2006) and come from a credible source (Wogalter & Mayhorn, 2008); and attract and maintain the attention of viewers through the use of signal words, such as ‘warning’ (Wogalter, Jarrard, & Simpson, 1992), alert icons or symbols, like ‘!’ (Ng & Chan, 2009; Wogalter, Conzola & Smith-Jackson, 2002) and colors (Leonard, 1999; Silic & Cyr, 2016). While much of this research has examined hard-copy messages in the physical environment, there is increasing interest in using online messages to warn users about activities such as: visiting malicious websites (Akhawe & Felt, 2013); disclosing personal information (Carpenter, Shreeves, Brown, et al., 2018); visiting pro-anorexia websites (Martijn, Smeets, Jansen, et al., 2009); gambling online (Gainsbury, Aro, Ball, et. al., 2015); pirating music (Ullman & Silver, 2018), attacking computer servers (Maimon, Alper, Sobesto & Cukier, 2014); and accessing legal pornography (Zaikina-Montgomery, 2011). There is to date, however, little research specifically examining the effectiveness of messages warning against accessing CSEM.

Online messages to prevent CSEM have been trialed by law enforcement agencies (e.g., Global Alliance Against Child Sexual Abuse Online, 2014) and are used by some Internet companies (e.g., Essers, 2013; Google, 2020). But without an evidence base as to their effectiveness their widespread use remains stalled (Prichard et al., 2019). CSEM-prevention messages have been recommended because they: (a) are consistent with health prevention models (Quayle & Koukopoulos, 2018); and (b) could be implemented by any agency with the capacity to inject code into HTML pages to trigger actions defined in the page’s java script (Prichard et al., 2019). Various agencies have this capacity, including P2P networks, Internet service providers, global search engines, media and communication regulatory bodies (e.g., Australia’s Office of the eSafety Commissioner), and law enforcement agencies (Prichard et al., 2019). Message functioning could also be written into Internet filtering software purchased by households, institutions (e.g., schools and universities) and any agency that provides publicly available Wi-Fi (e.g., fast food outlets, airports and public libraries).

Many approaches can be used to deliver messages to users. Messages can be activated when certain search terms are entered. They can also be activated when users attempt to access a URL known to contain CSEM. This is particularly important where URLs cannot be taken down because they do not exist on a centralized server, or because the URL uses bulletproof hosting or fast flux, which rapidly shuffle IP addresses for fully qualified domain names. Moreover, even where URL takedowns are effected, messages could still be activated usefully to communicate with users who have clicked on a link to the URL (i.e., before discovering the URL no longer exists), rather than them receiving the usual 404 error message.

From a situational crime prevention perspective, messages can serve several purposes. They may ‘increase the perceived risks’ of accessing CSEM by highlighting the chances and consequences of detection (while simply receiving a message reinforces the fact that activities online are perhaps not as anonymous as imagined) (Wortley & Smallbone, 2012). Alternatively, messages might ‘remove excuses’ by highlighting the harm suffered by the children depicted, as well as the potential harms to the viewer themselves (Williams, 2005). Some have argued that harm messages are likely to be more effective than deterrence messages because the latter might provoke defiant reactions against social control, or even increase users’ arousal and the excitement associated with CSEM (Williams, 2005; see also

Grabosky, 1996, p. 30). At this point, the question of which strategy is more effective – if indeed either are effective – is open.

Honeypots as a Research Tool

Most social science research on Internet behavior, including accessing CSEM, has relied on survey designs in which participants report on their online experiences or respond to hypothetical scenarios (e.g., Ullman & Silver, 2018; Zaikina-Montgomery, 2011). While informative, the limitations of such methods in terms of selection bias and ecological validity are well documented (e.g., Harrison, 1997). More recently, honeypots have been utilized as a method to directly observe deviant behavior online.

Honeypots are computers or Internet sites that mimic likely targets for online attacks or other deviant contact, and are thus used as 'bait' in order to detect, analyze and/or counter such unwanted activity. They are most commonly used in real world settings in the area of IT security (see Maimon, Kamerdze, Cukier & Sobesto, et al., 2013; Testa et al., 2017), but have sometimes been employed by law enforcement agencies to deter online child sexual exploitation offences (e.g., see Wortley & Smallbone, 2006a).

One of the first uses of an online honeypot as a social science research tool was by Demetriou and Silke (2003). They developed a website purporting to offer free legal games. When participants arrived at the landing page they discovered that website also offered (fake) links to hard-core pornography, soft-core pornography, and a range of illegal and pirated material. Over 88 days the honeypot received 803 visitors, 483 of whom attempted to access the fake hard-core pornography link, making it the most popular 'site', while the legal games link – the original reason that people visited the site – received just 268 clicks. The researchers used these results to theorize about the influence of anonymity on low-level deviant decision making.

Later researchers have conducted online experiments by systematically varying the information presented to participants. For example, Broadhurst and Jayawardene (2007) set up four fictitious accounts of 12-year-old children on three social network platforms. The profiles were varied on a number of dimensions, including whether or not there was an accompanying picture of the child. It was found that all profiles attracted suspicious contacts but there was variation among the profiles, with an accompanying picture increasing suspicious contacts.

Honeypot designs are not without limitations (Bossler, 2017; Holt, 2017; Steinmetz, 2017; Testa et al., 2017). In particular, it is usually not possible to collect personal data on participants (socio-demographics, psychological characteristics) to determine the nature of the sample or to analyze between-subject effects. Steps need to be taken to exclude multiple responses from the same individual and responses from bots (i.e., automated programs designed to mimic the behavior of Internet users). Also, because honeypots covertly observe participants' behavior without their consent ethical complexities can arise, especially when researchers are examining deviant or criminal behavior (Prichard et al., 2019). Against these limitations, honeypots offer a number of advantages over surveys. They involve the real-life behavior of individuals who are unaware that they are being observed, and thus are likely to have greater ecological validity. In addition, participants are self-selecting as to whether or not they visit the site and so issues of sampling bias may be minimized. Finally, honeypots offer the potential to carry out true experiments in which the researcher has control over the variables of interest.

The Current Study

The current study employed an online experiment utilizing a honeypot design to investigate the efficacy of warning messages as a prevention strategy for CSEM. Using situational crime prevention as our theoretical lens, our primary research question was whether online warning messages would dissuade individuals from attempting to proceed to the honeypot. The secondary question related to warning types, specifically whether harm or deterrence messages were the most effective.

Clearly, fake CSEM links in a honeypot study would be ethically, if not legally, problematic. Even though a fake CSEM link would not lead to any material, participants who clicked on it might nonetheless be guilty of an offence by attempting to access CSEM (Prichard et al., 2019). As a proxy for CSEM we used a form of pornography called ‘barely legal,’ also called ‘teen.’ This genre eroticises adult-minor sex. Although it is generally legal (see Ethics section below) and popular (Jensen, 2010; Pornhub, 2018), parts of the barely legal genre carry a higher deviant status than mainstream pornography because it employs various techniques to enhance the fantasy that an adult actress is a minor, such as: choosing actresses with small physical statures; clothing (e.g., pyjamas); child-like behaviour (e.g., giggling, shyness, crying); visual cues (e.g., apparent vaginal bleeding, teddy bears); themes (e.g., storylines involving step-fathers, babysitters, teachers); references to sexual inexperience (e.g., “fresh”, “innocent”, “virgin”); and the control exerted by male partners (Peters et al., 2014). The barely legal genre has even been described as “pseudo-child pornography” (Dines, 2009, p. 124).

As noted earlier, barely legal pornography has been also suggested as a pathway to CSEM. Most of the research in this area has involved surveys or qualitative case studies in which some offenders reported accessing barely legal pornography prior to accessing CSEM (Morgan & Lambie, 2018; Perkins & Wefers, 2019). Of course, showing that barely legal use predates CSEM use is does not of itself establish a causal link. In a rare experimental study, Paul and Linz (2008) provided empirical evidence that barely legal pornography may have a corrosive effect. They found that participants (undergraduate students) exposed to barely legal pornography were more likely to make cognitive associations between children and sexuality than participants shown adult pornography. Despite the limited research base, the available findings are consistent with theoretical models that portray involvement in CSEM use as becoming progressively more problematic over time through an iterative process of habituation and escalation (e.g., Fortin & Proulx, 2018; Paul & Linz, 2008; Quayle & Taylor, 2004).

METHOD

Design

We contracted an international website design and advertising company to assist with generating web traffic to our honeypot.[2] The commercial partner designed a fully functioning bodybuilding website, which we refer to here as *GetFit*. Visitors to *GetFit* are not aware that it is used for research purposes. *GetFit* contains articles on muscle development, sport, diet and some articles on sex, such as increasing male sexual performance through improving the strength of core muscles. The theme mimics www.menshealth.com and related sites. To enhance the realistic look and feel of the site, *GetFit* hosted eight real advertisements for, among other things, gym clothing, green tea, and dating websites.

During the experimental phase, *GetFit* contained fake advertisements (also called 'banners') for a pornography site, which we refer to here as *Just Barely Legal* (*JBL*). The adverts contained legally purchased non-pornographic images of models certified to be adults, accompanied with the text "Just Barely Legal*"* and an "enter" button. Participants who chose to click on the *JBL* advertisement were allocated to a control group or one of four experimental groups who received a message (2 x harm, 2 x deterrence). Allocation was randomized with *Mersene Twister*.

[2] Demetriou and Silke (2003) designed their honeypot in-house and successfully recruited their participants without strategies to draw web traffic, such as advertising. However, we carried out a pilot study that revealed this approach is no longer effective today because of (a) the size of the Internet and (b) users' expectations about contemporary web-design (e.g., Robins & Holmes, 2008).

The control group was taken straight to the JBL landing page. Experimental groups were presented with one of four messages relating to the risks of harm (to themselves or the ‘barely legal’ actresses) and police activity (surveillance or arrest). To comply with ethical requirements, all messages began with the same stem: “We thought you’d like to know this website shows females who are just above legal age, but may look younger”. The messages were initially pre-tested, through ratings of likely compliance with the warning by online panel survey participants, and were designed to be clear and concise as recommended by message-design literature (Laughery & Page-Smith, 2006):

- *Health professionals believe this material may lead users to become sexually aroused by children (H1);*
- *Health professionals believe the individuals shown may experience long-term feelings of distress (H2);*
- *Police may obtain IP addresses to track users (D1); and*
- *Viewing this material may be illegal in some countries and lead to arrest (D2)*[3].

The visual design of the messages incorporated the features found to increase the likelihood of compliance, including an alert symbol (!), and a signal word (‘warning’) (e.g., Ng & Chan, 2009). The messages were interstitial banners, which means that they covered users’ entire screen regardless of device type. This also meant that participants had to interact with the message, in some way, in order to remove it (e.g., by clicking ‘Exit’).

Since compliance with messages is affected by readers’ perceptions of the credibility of the source (Wogalter & Mayhorn, 2008), we chose to present the bodybuilding website as the author and source of the messages. Certainly, blank messages with no source would have been perceived as abnormal. Without a real agency that was willing to appear in the

[3] This statement is true. While in the US the legality of barely legal pornography is based on the actual age of the actors, in Australia, where the current research was carried out, the criterion of apparent age is used.

experiment as the source of the messages, our best option was to present *GetFit* as the source. Users had to get rid of the message by clicking ‘exit,’ ‘enter,’ or a navigation function (e.g., closing their browser). ‘Enter’ would direct users to the *JBL* landing page. ‘Exit’ would return them to *GetFit.*

The fake entrance page of *JBL* mimicked the layout and functionality of other pornography sites, providing users with the option of ‘exiting’ (navigating to the previous *GetFit* page) or ‘entering,’ which triggered a message after a 5s delay from *JBL*: “Sorry! We’re undergoing routine maintenance. Please check back shortly.” Control participants were directed to the *JBL* site without a message and had the same ‘enter/exit’ option.

The commercial partner maintained *GetFit* on Australian servers. It designed the *JBL* advert and website (constituting a single landing page). However, the *JBL* advertisements and the landing page were maintained by the researchers on two separate U.S. servers. This approach served two purposes. First, it ensured that meta-data for *GetFit* and *JBL* appeared unrelated, thereby avoiding suspicions about their authenticity. Secondly, the *JBL* website provided the platform through which experimental data about participants were stored and protected using a range of standard information security strategies, including: strong password protection on the virtualized servers, application servers and databases, and implementation of a 30 day password change policy; blocking of all incoming firewalls ports except port 80; deletion of any guest or non-authenticated accounts from the servers; the use of encrypted transports to move data to and from the servers; registration and payment of domain names for *JBL*, SSL certificates and virtualized server hosting using anonymized email addresses by an independent third party with no ties to the researchers; and monitoring of IP address server logs to ensure no unauthorized access had occurred.

By hosting the *GetFit* adverts on a separate server controlled by the researchers, only the researchers and not the commercial partner had access to IP addresses recorded in the experiment. Both *GetFit* and *JBL* were only accessible using SSL, using certificates issued by trusted third parties, giving the air of greater authenticity than non-SSL sites, and assuring users that the material they were accessing would not be transmitted "in the clear" over the internet.

Procedure

The *GetFit* website was launched on 6 April 2017 and at this point it could be visited by Internet users. On 27 November 2017 all aspects of the experiment began, including the *JBL* advert on *GetFit*, the warning message functions, the *JBL* landing page, and the data collection systems. The experiment was concluded on 2 April 2019. Because the experiment sought to circumvent observer effects, participants were not aware of their involvement in the study and did not provide consent. No identifying information was gathered about the participants other than IP addresses (although an IP to geographic location mapping is possible, and gathering browser metadata can be used to uniquely identify browsers). Social media advertising for *GetFit* was used to attract English-speaking Australian males aged 18-30 years to the website. The decision to limit the age range was made to maximise recruitment with our limited advertising funds; we determined that this age range would be the most likely to (a) respond to the *GetFit* advert and (b) click on the *JBL* advert. Restricting the age also simplified the creative website design process for our commercial partner – which chose the bodybuilding theme and generated the layout of *GetFit* to appeal to young adult males. Men were targeted because they are more likely than females to use pornography (Carroll et al., 2017; Rissel et al., 2017) and to have viewed a broader range of pornography (Svedin et al., 2011), like 'barely legal'. Concentrating on males also maximised the relevance of the findings to the context of CSEM-offending; most CSEM viewers appear to be male (see for instance Henshaw et al., 2017).

Outcome measures

We used Google Analytics to provide metrics about the numbers of visitors to *GetFit*, their pathway to the site, and their behavior at the site. With respect to our hypotheses, we measured whether the participants attempted to 'enter' the *JBL* website once they arrived at the landing page. This information was used to create a dichotomous dependent variable, *desistance*.

Manual checking was used to delete repetitions of IP addresses. Any records identified as bots were excluded. These steps reduced the risk of double counting and to ensure that each IP address represented an authentic, individual person. We could not prevent double counting if the same participant clicked on the *JBL* advert from different IP addresses (e.g., home and work). On the other hand, there may also be cases where the one IP address is used by multiple users, in which case there may be instances of unique participants being eliminated from the study.

Ethics

This experiment was approved by the University of Tasmania human research ethics committee (#H0012409) in accordance with international principles governing human research. Approval was granted because of the low risk of causing participants distress, participants' anonymity was adequately protected, no illegal behavior was observed and the research was for the public benefit. The message stem was required to ensure that the behavior of participants could not constitute an offence of attempting to view CSEM under Australian law (see further Prichard & Spiranovic, 2014, p. 7). Importantly, images of adult models used in this study were approved by the ethics committee to ensure that they complied with Australian CSEM criminal laws: the models did not objectively *appear* to be children. The images chosen to comply with laws and ethics requirements were necessarily 'conservative.'

RESULTS

According to Google Analytics, during the time that the experiment was conducted (6 April 2017 and 2 April 2019) *GetFit* was visited from 29,364 unique IP addresses. It seems likely that most of these IP addresses related to single individuals. However, it is not possible to discern how many visitors may have generated more than one IP address, for instance by visiting *GetFit* at work and then again at home. The mean time spent on *GetFit* was 12 seconds.

The bulk of visits (91.8%) originated through paid social media advertising. A further 3% (N=902) of visits occurred through social routes, such as shared links. 'Organic searches' – users finding *GetFit* via search engine queries – accounted for 2.6% of visits (N=763). The remaining 2.6% (N=784) of visits originated through other miscellaneous routes. The high percentage of traffic originating directly from paid social media advertising is important because the marketing was limited to (Australian) males aged between 18 and 30 years. In other words, we have a good degree of confidence that most visitors were young adult males. However, we acknowledge that some individuals may not be truthful about their age when signing up to social media.

The *JBL* advert received a total of 512 clicks. Data cleaning excluded repeat entries of IP addresses and non-human agents (e.g., bots). After this process the number of first-time clicks on *JBL* adverts from unique IP addresses was 419, representing 1.43% of *GetFit* visitors, a click through rate that is almost double the average of 0.77% for web-based display adverts (i.e., adverts for things people have not specifically searched for) (Irvine, 2020).

Desistance

Figure 1 presents the behaviour of the 419 participants who clicked on one of the *JBL* adverts. Notably the randomization function that we employed (*Mersene Twister*) meant that our cell sizes were uneven: 65 participants in the H2 group compared with 100 in the control. Of the 100 participants in the control group 73% attempted to gain access to the *JBL* site by clicking ‘enter’. This means that the control desistance rate was 27%.

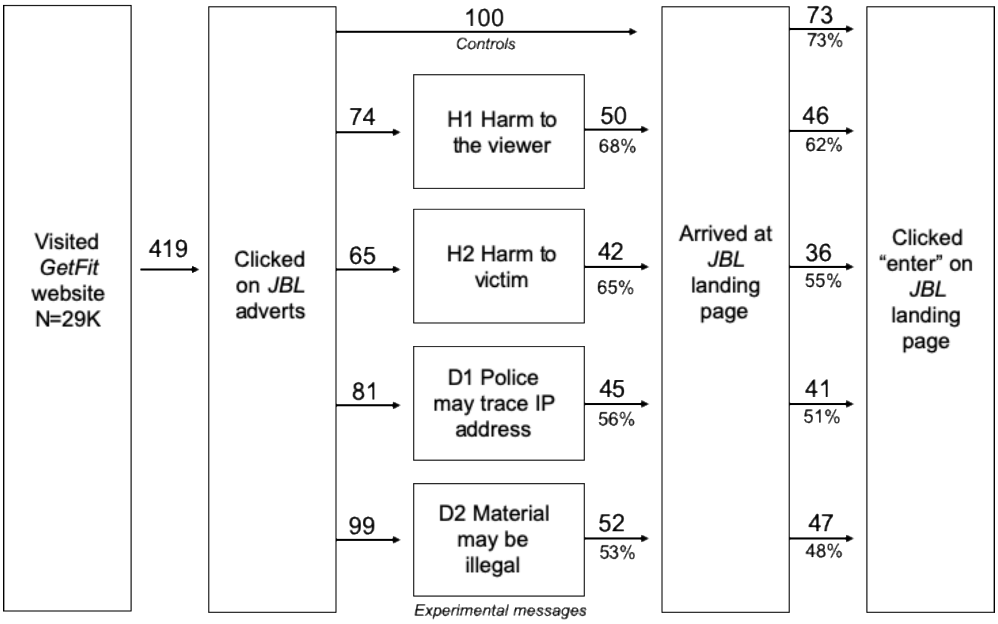

FIGURE 1 Numbers of participants who arrived at the *JBL* landing page and clicked ‘enter’ by condition type

Because the experimental groups received a warning message which prevented them from progressing to the *JBL* site until they confirmed their decision or navigated away, they had an additional opportunity for desistance. For example, after receiving their message, 24 of the H1 group decided not to visit the *JBL* landing page. However, of the 50 H1 participants who did decide to visit the *JBL* landing page, very few changed their minds: 46 clicked ‘enter’.

Four analyses were conducted, separately comparing each of the four experimental groups with the controls. Fisher's Exact Test (1-sided) was applied to determine the statistical significance of the observed proportion of users from each group who did not click ‘enter’ (i.e., desistance) on the JBL landing page.[4] A more stringent alpha level of .010 was adopted to establish statistical significance in order to reduce the possibility of type 1 error from conducting multiple comparisons.

Neither H1 [*p* = .087, *OR*= 1.65 (95% CI *OR* = 0.86, 3.14)] nor H2 [*p* = .015, *OR*= 2.18 (95% CI *OR* = 1.13, 4.21)] groups showed a significant difference, based on the more stringent alpha level of p<.010, in the desistance rates (i.e. proportion who did not click ‘enter’ on the JBL landing page) compared to the control group. The effect sizes were small but for the comparison involving H2, the odds ratio (OR = 2.18) met the threshold for a difference which is practically meaningful according to Ferguson’s (2009) guidelines for the social sciences.

For D1 and D2 groups, respective desistance rates were 49% and 52%, which are almost double that found for the control. Individual comparisons found that the difference between the control group and D1 [*p*= .002, *OR*= 2.64 (95% CI *OR* = 1.42, 4.90)] and D2 [(*p* < .001, *OR*= 2.99 (95% CI *OR* = 1.65, 5.41)] were statistically significant and practically meaningful.

For completeness, we followed up these analyses by examining the relationships among the four warning messages. None of the six pairwise comparisons were significant at p<.010.

DISCUSSION

We investigated two research questions: Do warning messages immediately influence the behavior of users attempting to access barely legal pornography? And do effects

[4] In contrast to Chi-Square, there is no statistical test value to report when conducting the Fisher's Exact Test.

vary according to whether messages focus on deterrence, or the harms associated with viewing such pornography? We found that deterrence-focussed online warning messages significantly reduced the click-through to the barely legal pornography site. This finding does not support Williams' (2005) concern that CSEM-deterrent messages might be counterproductive because they could provoke defiant reactions against social control, or make CSEM seem more alluring to users. Rather, our results support Wortley and Smallbone's (2012) assertion that deterrent messages may dissuade some users from accessing CSEM by increasing the perceived risks associated with this crime. However, we also found that harm-focussed messages had no significant impact on the click-through rate to the barely legal pornography site. This result is inconsistent with predictions made by both Williams (2005) and Wortley and Smallbone (2012).

The current study is one of the few, though growing, number of studies utilising experimental designs to examine behaviour on the Internet. The development of our *GetFit* website was labour-intensive because its ultimate purpose was to provide a realistic Internet experience for the participants. The majority of them had clicked on a social media advert to visit an information-rich professionally designed website on male fitness. There, among other adverts, participants might see and decide to click on an advert for barely legal pornography. This unsolicited opportunity mirrored opportunities that some Internet users encounter to view CSEM.

Waiting for participants to self-select in this way took approximately 16 months (ie 27 November 2017 to 2 April 2019). Although slow, the benefit of this approach is that we have confidence that the participants who clicked on the *JBL* advert were naïve and exhibited real-life behaviours. Since the participants were randomly allocated to one of the five conditions (control and four experimental groups), it can be assumed that differences between the groups was not due to a selection bias or other factors. It is also relevant to note that

GetFit has a 'contact us' email address which was monitored by the commercial partner. This email account did not receive any complaints about the functioning of *GetFit* or *JBL*, despite the latter's repeated error message about "undergoing routine maintenance". Nor were any system trespass (hacking) attempts made on *GetFit* or *JBL*. These facts can be interpreted to mean that none of the users suspected the true research purposes of the sites.

Notwithstanding these strengths, our study shares the limitations of other honeypot studies. Without demographic data on participants we have no way to check the composition of the sample. While our social media advertising targeted males between the ages of 18-30, we cannot be certain that our sample does not include some younger or older participants, or females. Likewise, while we made efforts to ensure that only first time IP addresses appeared in our database, it is possible that some participants were counted more than once because they accessed the *JBL* advert from different IP addresses. Conversely, since a single IP may be shared by many individuals, it is possible that we excluded some naïve participants and thus reduced our sample size. Overall, however, we would expect the effects of these issues to be minimal and a reasonable trade-off for the benefits the honeypot design offers.

More pertinently, we acknowledge a number of limitations specifically related to the way that messaging in the study was implemented. First, there are possible issues with the authoritativeness of our messages. We chose to present the *GetFit* website as the source of the warning messages because we determined that a 'blank' message without an identified source would be suspicious and untrustworthy in the context of an interrupted visit to a pornography website. While *GetFit* might have been better than no source, it is debatable how credible participants perceived it to be. This is an important consideration given that source credibility is a motivator for warning compliance (Wogalter & Mayhorn, 2008).

A second limitation was that for our project to comply with Australian law and research ethics, all four messages began with the same stem: "We thought you'd like to know this website shows females who are just above legal age, but may look younger.” The stem may have reduced the efficacy of all message conditions because it reduced conciseness. Instead of only reading the 8 -14 words contained the message types, the participants first had to read 20 words of text contained in the stem about something that they probably already knew: that *JBL* was promising images of women just over the age of consent.

Third, the low deviancy portrayed by the *JBL* advert may have caused some participants not to believe the messages, believability (not surprisingly) being related to message-compliance (e.g., Riley, 2014). According to our commercial partner, which assayed the types of adverts pornography companies use in real life, the image used in this study for the *JBL* advert was conservative. In criminological terms the image projected low deviancy because, among other things, the *JBL* advert did not give any indication that it would lead to pornography that incorporated any of the techniques catalogued by Peters et al. (2014) to eroticise the fantasy of adult-minor sex. For example, the adult model does not have a small physical stature, there are no child-props such as teddy bears, she faces the camera in a confident way and does not exhibit child-like behaviours such as shyness, and the text in the advert made no reference to sexual inexperience (e.g., “innocent”, “fresh”, “virgin”) or adult-minor themes (e.g., step-fathers, babysitters). In these circumstances, participants may well have asked themselves why police would waste time tracking IP addresses of people using mainstream pornography, or how viewing the *JBL* material could “lead users to become sexually aroused by children”.

It is important to note that the most likely effect of these limitations is to make it more difficult to find significant effects, and thus, if anything, increases our confidence in the results. The fact that any sort of automated message worked to reduce access to *JBL* ought to be of great interest to law enforcement agencies and others concerned with preventing CSEM. It is argued that the effects we observed would be considerably stronger if messages were genuinely applied to prevent CSEM-onset. Problems with credibility or believability would largely disappear. Internet users would unquestionably find an agency such as the Federal Bureau of Investigation a more credible source of information than an obscure fitness website. Equally, Internet users who had knowingly clicked on a link leading to CSEM would be much more inclined to believe messages about, for instance, law enforcement surveillance, the material's illegality, and potential harmfulness.

Our findings provide further support for applying situational crime prevention to the problem of CSEM (Smallbone & Wortley, 2017; Wortley, 2012; Wortley & Smallbone, 2012). However, we are not claiming that warning messages will necessarily have a long-term impact on the behavior of all potential first-time offenders. The question as to whether users might displace to other sites or habituate to CSEM warning messages over time are among a number of research questions worth interrogating empirically at a future date. But it would be premature at this stage to assume that offender adaptation would ultimately make CSEM warnings futile. Since CSEM-messaging could reach hundreds of thousands of potential new users, it seems feasible that a useful proportion of them could indeed be convinced to never again attempt to access the material, particularly if their original attempt was only made "impulsively and/or out of curiosity" (Beech et al., 2008, p. 255). There is hardly a shortage of genres of legal pornography for such individuals to explore (e.g., Pornhub, 2018). Additionally, evidence from other fields indicates that human reaction to repeat message exposure is not necessarily habitual; decision-making is influenced by the specific circumstances of each message (Reeder et al., 2018, p. 9).

Our study also adds to the broader literature on warning messages and, in turn, further exploration of the issue can be guided by that research base. Notwithstanding the limitations we have acknowledged, we have shown that warning messages, delivered at the time that the individual is considering engaging in the activity in question, can significantly influence their decision making and deter them from proceeding. As we have noted, a replication using messages from a more authoritative source is a priority (Riley, 2006; Wogalter & Mayhorn, 2008). Worthwhile avenues to examine also include the physical presentation of the message – for example, the use of images, audio, and animation – to attract the viewer's attention (Leonard, 1999; Ng & Chan, 2009; Silic & Cyr, 2016; Wogalter, et al., 2002).

We conclude with a broader comment about the implications of our study. We agree with scholars in a variety of fields, including the physical and life sciences (Ledford, 2015) and criminology (Henry, 2012), who see interdisciplinary research as essential to solve many of the world's most complex problems. The present study on one complex form of cybercrime, CSEM, could not have succeeded without sustained collaboration between criminologists, IT experts, psychologists, criminal lawyers, and non-academic commercial partners. Perhaps where cybercrime is concerned criminologists should not be expected to be "lighthouses that provide light and direction in uncertain, dark, and stormy times when little is known about a phenomenon and how to address it" (Bossler, 2017, p. 681), but simply experts who can make valuable contributions within interdisciplinary teams.

ACKNOWLEDGMENTS

The authors take responsibility for the integrity of the data, the accuracy of the data analyses, and have made every effort to avoid inflating statistically significant results.

DISCLOSURE OF FINANCIAL INTERESTS

The authors declare no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

FUNDING

This project was funded by the Australian Government through the Australian Research Council (DP160100601).

ORCID iD

Jeremy Prichard 0000-0002-8481-7100

Richard Wortley 0000-0003-0319-7163

Paul A. Watters 0000-0002-1399-7175

Caroline Spiranovic 0000-0002-5270-8719

Tony Krone 0000-0001-6362-7925

REFERENCES

Akhawe, D., & Felt, A. P. (2013) *Alice in warningland: A large-scale field study of browser security warning effectiveness*. Paper presented at the 22nd USENIX Security Symposium. https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_akhawe.pdf

Beech, A. R., Elliott, I. A., Birgden, A., & Findlater, D. (2008). The Internet and child sexual offending: A criminological review. *Aggression and Violent Behavior, 13*(3), 216-228. https://doi:10.1016/j.avb.2008.03.007

Bossler, A. M. (2017). Need for debate on the implications of honeypot data for restrictive deterrence policies in cyberspace. *Criminology & Public Policy, 16*(3), 681-688. https://doi.org/10.1111/1745-9133.12322

Broadhurst, R., & Jayawardene, K. (2007). Online Child Sex Solicitation: Exploring the feasibility of a research 'sting'. *International Journal of Cyber Criminology*, *1*(2), 228-248.

Carpenter, S., Shreeves, M., Brown, P., Zhu, F., & Zeng, M. (2018). Designing warnings to reduce identity disclosure. *International Journal of Human–Computer Interaction, 34*(11), 1077-1084. https://doi.org/10.1080/10447318.2017.1413792

Carroll, J. S., Busby, D. M., Willoughby, B. J., & Brown, C. C. (2017). The porn gap: Differences in men's and women's pornography patterns in couple relationships. *Journal of Couple & Relationship Therapy, 2,* 146-163. https://doi.org/10.1080/15332691.2016.1238796

Child Dignity Alliance. (2018). *Technology working group report*. London: Child Dignity Alliance.

Clarke, R.V. (2017). 'Situational crime prevention'. In R. Wortley & M. Townsley, M. (eds). *Environmental Criminology and Crime Analysis* (2nd ed). London: Routledge.

Demetriou, C., & Silke, A. (2003). A criminological Internet 'sting': Experimental evidence of illegal and deviant visits to a website trap. *British Journal of Criminology, 43*(1), 213-222. https://doi:10.1093/bjc/43.1.213

Dines, G. (2009). Childified women: How the mainstream porn industry sells child pornography to men. In S. Olfman (Ed.), *The sexualization of childhood* (pp. 121-142). Westport, CT: Praeger.

Essers, L. (2013). Google to warn users of 13,000 search terms associated with child pornography. PCWorld. https://www.pcworld.com/article/2064520/google-to-warn-users-of-13000-search-terms-associated-with-child-pornography.html

Ferguson, C. J. (2009). An effect size primer: A guide for clinicians and researchers. *Professional Psychology: Research and Practice, 5*, 532-538. http://dx.doi.org/10.1037/a0015808

Fortin, F., & Proulx, J. (2019). Sexual interests of child sexual exploitation material (CSEM) consumers: four patterns of severity over time. *International journal of offender therapy and comparative criminology, 63*(1), 55-76. https://doi.org/10.1177/0306624X18794135

Gainsbury, S., Aro, D., Ball, D., Tobar, C., & Russell, A. (2015). Determining optimal placement for pop-up messages: Evaluation of a live trial of dynamic warning messages for electronic gaming machines. *International Gambling Studies, 15*(1), 141-158. https://doi.org/10.1080/14459795.2014.1000358

Global Alliance Against Child Sexual Abuse Online. (2014). Norway. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/docs/reports-2014/ga_report_2014_-_norway_en.pdf

Google. (2020). Fighting child sexual abuse online. https://protectingchildren.google/intl/en/

Grabosky, P. N. (1996). *Unintended consequences of crime prevention.* In Crime Prevention Studies.

Harrison, L. (1997). The validity of self-reported drug use in survey research: an overview and critique of research methods. *NIDA research monograph, 167*, 17-36.

Henry, S. (2012). Expanding our thinking on theorizing criminology and criminal justice? The place of evolutionary perspectives in integrative criminological theory. *Journal of Theoretical and Philosophical Criminology, 4*(1), 62-89.

Henshaw, M., Ogloff, J. R. P., & Clough, J. A. (2017). Looking beyond the screen: A critical review of the literature on the online child pornography offender. *Sexual Abuse: Journal of Research and Treatment*, *29*(5), 416-445. https://doi:10.1177/1079063215603690

Henzey, M. J. (2011). Going on the offensive: A comprehensive overview of Internet child pornography distribution and aggressive legal action. *Appalachian Journal of Law, 11*, 1-70.

Holt, T. J. (2017). On the value of honeypots to produce policy recommendations. *Criminology & Public Policy*, *16*(3), 739-747. https://doi.org/10.1111/1745-9133.12315

Home Affairs Committee. (2018). Policing for the future: Report. House of Commons: United Kingdom.

Internet Watch Foundation. (2017). *Annual report 2017*. https://www.iwf.org.uk/sites/default/files/reports/2018-04/IWF%202017%20Annual%20Report%20for%20web_0.pdf

Irvine, M. (2020). *Google Ads Benchmarks for YOUR Industry*. The WordStream Blog. https://www.wordstream.com/blog/ws/2016/02/29/google-adwords-industry-benchmarks

Jensen, R. E. (2010). A content analysis of youth sexualized language and imagery in adult film packaging, 1995–2007. *Journal of Children and Media, 4*(4), 371-386. https://doi.org/10.1080/17482798.2010.510005

Krone, T. (2004). *A typology of online child pornography offending*. Canberra: Australian Institute of Criminology.

Lanning, K. V. (2010). Child molesters: A behavioral analysis for professionals investigating the sexual exploitation of children (5th ed., pp. 1-212): National Center for Missing & Exploited Children.

Laughery, K., & Page-Smith, K. (2006). Explicit information in warnings. In M. S. Wogalter (Ed.), *Handbook of warnings* (pp. 419-428). Mahwah, NJ: Lawrence Erlbaum Associates Inc.

Ledford, H. (2015). How to solve the world's biggest problems. *Nature News* (7569), 308. https://doi:10.1038/525308a

Lenorovitz, D. R., Leonard, S. D., & Karnes, E. W. (2012). Ratings checklist for warnings: a prototype tool to aid experts in the adequacy evaluation of proposed or existing warnings. *Work, 41* (Supplement 1), 3616-3623.

Long, M., Alison, L., Tejeiro, R., Hendricks, E., & Giles, S. (2016). KIRAT: Law enforcement's prioritization tool for investigating indecent image offenders. *Psychology, Public Policy, and Law, 22*(1), 12–21. https://doi.org/10.1037/law0000069

Ly, T., Dwyer, R. G., & Fedoroff, J. P. (2018). Characteristics and treatment of internet child pornography offenders. *Behavioral Sciences and the Law, 36*(2), 216-234. https://doi:10.1002/bsl.2340

Maimon, D., Alper, M., Sobesto, B., & Cukier, M. (2014). Restrictive deterrent effects of a warning banner in an attacked computer system. *Criminology, 52*(1), 33-59. https://doi:10.1111/1745-9125.12028

Maimon, D., Kamerdze, A., Cukier, M., & Sobesto, B. (2013). Daily trends and origin of computer-focused crimes against a large university computer network: An application of the routine-activities and lifestyle perspective. *The British Journal of Criminology, 53*(2), 319-343. https://doi:10.1093/bjc/azs067

Martijn, C., Smeets, E., Jansen, A., Hoeymans, N., & Schoemaker, C. (2009). Don't get the message: the effect of a warning text before visiting a proanorexia website. *International Journal of Eating Disorders, 42*(2), 139-145. https://doi.org/10.1002/eat.20598

Mayhew, P., Clarke, R. V. G., Sturman, A., & Hough, J. M. (1975). *Crime as Opportunity*. London: Home Office Research and Planning Unit.

Merdian, H. L., Perkins, D. E., Dustagheer, E., & Glorney, E. (2018). Development of a case formulation model for individuals who have viewed, distributed, and/or shared child sexual exploitation material. *International Journal of Offender Therapy and Comparative Criminology*, 1-19. https://doi:10.1177/0306624X17748067

Merdian, H. L., Wilson, N., & Boer, D. P. (2009). Characteristics of Internet sexual offenders: A review. *Sexual Abuse in Australia and New Zealand, 2*(1), 34-45.

Morgan, S., & Lambie, I. (2019). Understanding men who access sexualised images of children: exploratory interviews with offenders. *Journal of Sexual Aggression, 25*(1), 60-73. https://doi.org/10.1080/13552600.2018.1551502

Ng, A. W., & Chan, A. H. (2009). *What makes an icon effective?* AIP Conference Proceedings.

Paul, B & Linz, D.G. (2008), The effects of exposure to virtual child pornography on viewer cognitions and attitudes toward deviant sexual behavior, *Communication Research*, 35(1), 3-38.

Perkins, D., & Wefers, S. (2019). Treatment of Internet-related sexual offenders. In J.L. Ireland, C.A. Ireland & P Birch (eds) *Violent and Sexual Offenders: Assessment, Treatment and Management (2nd ed).* Abingdon, Oxon: Routledge.

Peters, E. M., Morrison, T., McDermott, D. T., Bishop, C. J., & Kiss, M. (2014). Age is in the eye of the beholder: Examining the cues employed to construct the illusion of youth in teen pornography. *Sexuality and Culture, 18*(3), 527-546. https://doi:10.1007/s12119-013-9210-5

Pornhub. (2018). 2018 Year in review. https://www.pornhub.com/insights/2018-year-in-review

Prichard, J., Krone, T., Spiranovic, C., & Watters, P. (2019). Transdisciplinary research in virtual space: can online warning messages reduce engagement with child exploitation material? In R. Wortley, A. Sidebottom, N. Tilley & G. Laycock (Eds.), *Routledge handbook of crime science*: Routledge.

Prichard, J., & Spiranovic, C. (2014). Child exploitation material in the context of institutional child sexual abuse. Sydney: Royal Commission into Institutional Responses to Child Sexual Abuse.

Prichard, J., Spiranovic, C., Watters, P., & Lueg, C. (2013). Young people, child pornography, and sub cultural norms on the Internet. *Journal of the American Society for Information Science and Technology, 64*(5), 992-1000. https://doi.org/10.1002/asi.22816

Prichard, J., Watters, P. A., & Spiranovic, C. (2011). Internet subcultures and pathways to the use of child pornography. *Computer Law and Security Review*, *27*(6), 585-600. https://doi:10.1016/j.clsr.2011.09.009

Quayle, E. (2012). Organisational issues and new technologies. In M. Erooga (Ed.), *Creating safer organisations: practical steps to prevent the abuse of children by those working with them*. Chichester: Wiley-Blackwell.

Quayle, E., Jonsson, L. S., Cooper, K., Traynor, J., & Svedin, C. G. (2018). Children in identified sexual images – Who are they? Self- and non-self-taken images in the International Child Sexual Exploitation Image Database 2006–2015. *Child Abuse Review, 27*(3), 223-238. https://doi:10.1002/car.2507

Quayle, E., & Koukopoulos, N. (2018). Deterrence of online child sexual abuse and exploitation. *Policing* (June), pp. 1-18. https://doi:10.1093/police/pay028

Quayle, E., & Taylor, M. (2004). *Child pornography: An internet crime*. Abington, Oxon: Routledge.

Reeder, R. W., Felt, A. P., Consolvo, S., Malkin, N., Thompson, C., & Egelman, S. (2018) *An experience sampling study of user reactions to browser warnings in the field*. Paper presented at the Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems.

Riley, D. (2014). Mental models in warnings message design: A review and two case studies. *Safety Science, 61*, 11-20. https://doi.org/10.1016/j.ssci.2013.07.009

Rissel, C., Richters, J., Visser, R. O. D., McKee, A., Yeung, A., & Caruana, T. (2017). A profile of pornography users in Australia: Findings from the second Australian study of health and relationships. *The Journal of Sex Research*, *2*, 227-240. https://doi.org/10.1080/00224499.2016.1191597

Robins, D., & Holmes, J. (2008). Aesthetics and credibility in web site design. *Information Processing & Management*, *44*(1), 386-399. https://doi.org/10.1016/j.ipm.2007.02.003

Rushkoff, D. (2009). The Web's dirtiest site. Retrieved 1 July 2019 from www.thedailybeast.com/blogs-and-stories/2009-08-11/the-webs-dirtiest-site.

Seto, M. C. (2013). Internet sex offenders. Washington, DC: American Psychological Association. http://dx.doi.org/10.1037/14191-000

Seto, M. C. (2019). The motivation-facilitation model of sexual offending. *Sexual Abuse*, *31*(1), 3-24.

Silic, M., & Cyr, D. (2016). *Colour arousal effect on users' decision-making processes in the warning message context.* International Conference on HCI in Business, Government, and Organizations. https://www.alexandria.unisg.ch/248785/1/Colour%20arousal%20effect%20on%20users%E2%80%99%20decision-making%20processes%20in%20the%20warning%20message%20context.pdf

Seto, M. C., & Eke, A. W. (2015). Predicting recidivism among adult male child pornography offenders: Development of the Child Pornography Offender Risk Tool (CPORT). *Law and human behavior*, *39*(4), 416.

Smallbone, S., & Wortley, R. (2017). Preventing child sexual abuse online. In J. Brown (Ed.), *Online risk to children: impact, protection and prevention*. London: John Wiley & Sons.

Steinmetz, K. F. (2017). Ruminations on warning banners, deterrence, and system intrusion research. *Criminology & Pub. Pol'y*, *16*, 725.

Svedin, C. G., Åkerman, I., & Priebe, G. (2011). Frequent users of pornography. A population based epidemiological study of Swedish male adolescents. *Journal of Adolescence, 34*(4), 779-788. https://doi:10.1016/j.adolescence.2010.04.010

Taylor, M., & Quayle, E. (2008). Criminogenic qualities of the Internet in the collection and distribution of abuse images of children. *Irish Journal of Psychology, 29*(1-2), 119-130. https://doi:10.1080/03033910.2008.10446278

Testa, A., Maimon, D., Sobesto, B., & Cukier, M. (2017). Illegal roaming and file manipulation on target computers: Assessing the effect of sanction threats on system trespassers' online behaviors. *Criminology and Public Policy, 16*(3), 689-726. https://doi:10.1111/1745-9133.12312

Ullman, J. R., & Silver, N. C. (2018). *Perceived effectiveness of potential music piracy warnings.* Proceedings of the Human Factors and Ergonomics Society Annual Meeting.

We Protect (2019). *Global threat assessment 2019: Working together to end the sexual exploitaiton of children online*. London: Open Government Licence. https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/5deecb0fc4c5ef23016423cf/1575930642519/FINAL+-+Global+Threat+Assessment.pdf

Williams, K. S. (2005). Facilitating safer choices: Use of warnings to dissuade viewing of pornography on the internet. *Child Abuse Review, 14*(6), 415-429. https://doi:10.1002/car.920

Wilson, T., Maimon, D., Sobesto, B., & Cukier, M. (2015). The effect of a surveillance banner in an attacked computer system: Additional evidence for the relevance of restrictive deterrence in cyberspace. *Journal of Research in Crime and Delinquency, 52*(6), 829-855. https://doi.org/10.1177/0022427815587761

Wogalter, M. S., Conzola, V. C., & Smith-Jackson, T. L. (2002). Research-based guidelines for warning design and evaluation. *Applied Ergonomics*, *33*(3), 219-230. https://doi.org/10.1016/S0003-6870(02)00009-1

Wogalter, M. S., Jarrard, S. W., & Simpson, S. N. (1992). *Effects of warning signal words on consumer-product hazard perceptions.* Proceedings of the Human Factors and Ergonomics Society Annual Meeting.

Wogalter, M. S., & Mayhorn, C. B. (2008). Trusting the internet: Cues affecting perceived credibility. *International Journal of Technology and Human Interaction (IJTHI)*, *4*(1), 75-93. https://doi.org/10.4018/jthi.2008010105

Wortley, R. (2012). Situational prevention of child abuse in the new technologies. In K. Ribisl & E. Quayle (Eds.), *Preventing online exploitation of children* (pp. 1-28). London: Routledge.

Wortley, R. & Smallbone, S. (2006a). *Child pornography on the Internet. Problem-Oriented Guides for Police Series.* Washington DC: U.S. Department of Justice. https://popcenter.asu.edu/content/child-pornography-internet-0

Wortley, R., & Smallbone, S. (2006b). Applying situational principles to sexual offenses against children. In R. Wortley & S. Smallbone (Eds.), *Situational prevention of child sexual abuse* (Vol. 19, pp. 7-35). Morsey NY: Criminal Justice Press.

Wortley, R., & Smallbone, S. (2012). *Internet child pornography: Causes, investigation, and prevention*: ABC-CLIO.

Zaikina-Montgomery, H. (2011). *The dilemma of minors' access to adult content on the internet: A proposed warnings solution* (PhD). University of Nevada, Las Vegas.