Naïve participants in online studies: can research ethically include participants without their consent?

Jeremy Prichard
Law School
University of Tasmania
Bag 89, Hobart 7001
jeremy.prichard@utas.edu.au

Caroline Spiranovic
Law School
University of Tasmania
Bag 89, Hobart 7001
caroline.spiranovic@utas.edu.au

Christopher Lueg
School of Engineering & ICT
University of Tasmania
Bag 87, Hobart 7001
christopher.lueg@utas.edu.au

ABSTRACT
Like the social sciences, much HCI research depends upon securing informed consent from participants prior to their inclusion in research designs. Among other things, when researchers seek informed consent they are adhering to the ethical principle that research should not interfere with, nor disrespect the autonomy of individuals. Drawing on principles from Australia's *National Statement on Ethical Conduct in Human Research*, this paper examines situations in which participants' consent may be waived. In this paper we discuss a case study of an interdisciplinary HCI and Criminology project which was granted approval from a registered human research ethics committee. The project conducted a randomised-controlled-experiment with naïve participants to examine the influence of pop-up messages on the use of deviant legal pornography in the broader context of addressing the online sharing of Child exploitation material (CEM).

Author Keywords
research ethics, ethics approval, online behaviour,

ACM Classification Keywords
H5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous.

INTRODUCTION
Child exploitation material (CEM), frequently misnomed 'child pornography', is an international phenomenon that presents complex problems to policy makers, law enforcement agencies, and other stakeholders. Although global definitions of CEM are inconsistent, in the main CEM refers to material depicting children of all ages – including infants – engaged in a continuum of activities ranging from sexual posing through to rape, torture, and bestiality (Niveau, 2010).

Children abused in the production of CEM can be physically harmed from sexual penetration and/or torture. Many are traumatised by the knowledge that records of their abuse are repeatedly accessed online for the sexual stimulation of others, or to 'groom' other children into sexual activity with adults (Prichard, Watters & Spiranovic, 2011). With continual advances in Internet capability, the CEM market is experiencing a boom in demand and supply (O'Donnell & Milner, 2007). For instance, one European website that operated for 76 hours with 99 CEM images received in excess of 12 million hits, including 2,800 from Australia (Allard, 2008). Public concern about CEM is high. High profile prosecutions for accessing CEM have involved Andy Muirhead (ABC TV presenter), Patrick Power (Senior Prosecutor NSW), and Neil Williams (VIC QC).

International efforts to counter the CEM market rely almost exclusively on law enforcement agencies to detect and prosecute offenders for CEM production, distribution and possession.

We were particularly interested in empirical evidence suggesting that a proportion of CEM is not accessed or shared by actual child abusers or by people with a pre-existing sexual interest in children, but by previously law-abiding people drawn to such material out of curiosity and/or impulsivity (Wortley, 2012: 193). We speculated that reducing the prevalence of CEM and related materials on certain file sharing web sites would be possible and would serve two important purposes:

1. *Reducing the continuous harm to victims* of abuse that is caused by sharing images of their abuse for fun and/or sexual gratification

2. *Reducing the value of CEM as a 'trading commodity'* on certain file sharing web sites, therefore also *increasing the barriers to accessing CEM*

In the research reported in this paper we sought to explore what might be called a 'second chance' approach which would rely on informing naïve participants about what they were about to do, i.e., accessing CEM, and potential legal ramifications thereof.

STUDY DESIGN
The study design drew from two research domains, criminology and human computer interaction.

The methodology for the study drew on the research of criminologists Demetriou and Silke (2003). They used a live study website that advertised freeware/shareware and that also contained fake links to illegal material to allow

OzCHI '15 , December 07 - 10 2015, Melbourne, VIC, Australia
Copyright © 2015 ACM 978-1-4503-3673-4/15/12... $15.00
http://dx.doi.org/xx.xxxx/xxxxxxx.xxxxxxx.

the researchers to estimate the proportion of users who would attempt to access such material. Using a similar website with fake links to legal pornography, our study was set up to test whether pop-up messages would alter pornography usage. It would also test William's (2005) view that legal/deterrent-focused messages will be less effective than harm-focused messages. Legal and ethical boundaries precluded this project from directly studying CEM. Instead this project focused on a closely related category of *legal* pornography, called "barely legal" or "teen". We considered "barely legal" a useful proxy for CEM because of its detailed focus on adult-minor sex. Indeed, Dines (2009:124) refers to "barely legal" as "pseudo-child pornography".

Taylor and Quayle (2008) suggested that pop-up messages could be linked with CEM search terms, highlighting the illegal status of the material. However, drawing on epidemiological studies of the effectiveness of health warnings, Williams (2005) explained that the impact of pop-up messages might depend to a large degree on their format and structure. She argued that legal, official warnings might paradoxically increase the likelihood that CEM is accessed. This is because they (a) magnify the deviant status and attractiveness of CEM, or (b) are perceived as a shallow threat to Internet freedoms. Williams (2005: 425) suggested that pop-up messages that explained the harms involved in producing and viewing CEM would be more effective in altering behaviour. These hypotheses have not been empirically tested.

The HCI specific contribution to the project was in the different ways of interacting with warning messages and pop-up messages in particular. The effectiveness of browser warnings had been investigated but only in the context of online security where security toolbars in a web browser would show security-related information about a website to help users detect likely phishing attacks. Phishing attacks use email or malicious web sites pretending to be trustworthy, often by copying the layout of trusted web sites, to solicit personal, often financial, information.

Wu et al (2006) argue that "because the [security] toolbars are designed for humans to use, they should be evaluated for usability -- that is, whether these toolbars really prevent users from being tricked into providing personal information". They found that "even though subjects were asked to pay attention to the security toolbar, many failed to look at it". In the context of our CEM research it was particularly interesting that "others disregarded or explained away the toolbars' warnings if the content of web pages looked legitimate". Egelman et al (2008) reported a significantly higher success rate when using active warning i.e., "warnings which force users to notice the warnings by interrupting them."

In what follows we will focus on the ethical considerations guiding this research, not the practicalities of the research.

RESEARCH ETHICS

Australia's National Statement on Ethical Conduct in Human Research defines 'human research' broadly to encompass among other things the observation of people, analysis of individuals' personal documents and information, surveys, interviews, psychological or medical treatment, and analysis of human tissue (NHMRC, 2007:7). Human research, therefore, is one of the defining features of academia; it is undertaken by a very wide array of academic disciplines – the medical sciences, epidemiology, the social sciences, law, criminology and computing, including human-computer interaction (HCI). The National Statement, like other documents that regulate research internationally, recognises cornerstone ethical principles for human research. One of these cornerstones is the principle of respect for individual autonomy. When researchers seek informed consent from individuals they are respecting their autonomy by, axiomatically, permitting them to choose whether to participate in a study. Other key principles are non-maleficence (avoiding harm) and beneficence (benefitting participants and the community).

Ethical principles governing research are not static or formulaic; they are used to assess the ethical merits and flaws in research designs.

The interdisciplinary criminology/HCI project which is the focus of this paper aimed to conduct an online randomised-controlled trial (RCT) with naïve participants – observing their behaviour without their consent. Importantly, ethics approval has already granted to this project by a registered Human Research Ethics Committee (HREC). The rationale for ethics approval is explained and, in the final part, the paper discusses the implications of this case study for future online HCI studies with RCTs involving naïve participants.

Under the National Statement, a waiver of consent may be justified if the reasons for the waiver are consistent with section NS §2.3. Specifically, according to section to 2.3.6 of the National Statement, an ethics committee may waiver consent on the grounds that:

- The study involves low risk to participants (2.3.6(a)) as there is no foreseeable harm or discomfort to participants
- The benefits of the research justify the harms associated with not seeking consent (2.3.6(b))
- It is impractical for justifiable reasons to obtain consent (2.3.6(c))
- There is no reason to believe that participants would not have consented to participating had they been asked (2.3.6(d))
- There are procedures and safeguards in place to ensure the privacy of participants and confidentiality is protected (2.3.6(e) & (f))

- There is a plan for making the result of the research available to participants should the outcomes of the research have the potential to influence the welfare of participants (2.3.6(g)).

- There is no possibility of commercial exploitation of data generated by the study which may deprive participants of financial benefits to which they are entitled (2.3.6(h)) and

- The waiver is not prohibited by law (state, federal or international) (2.3.6(i)).

A waiver of consent is commonly sought in secondary research projects involving retrospective databases such as Electronic Health Records (EHR) and crime databases. In the case of secondary research involving EHRs, privacy, autonomy and consent are two major and closely linked ethical considerations (Jensen et al., 2012). Elger and colleagues (2010) note that it is possible, in a number of countries, to seek a waiver of informed consent in research where for instance the purposes of the study are not incompatible with the initial purposes specified for data collection, results of the study are of substantial public interest and/or where it would be unreasonable, impractical or impossible to retrospectively contact participants to obtain consent. It has also been suggested that EHR researchers can argue that an inflexible requirement for consent would lead to biases in sample selection (Willison, 2005).

In the case of secondary research involving crime databases, it is common in particular for a waiver of consent to be sought and granted for research using offender recidivism databases. To the best of the authors' knowledge, there are no known population-based studies of offender recidivism that have required consent due to the need for unbiased data from the total population (as opposed to a sample of the population) and the prohibitive costs and time involved in tracing and contacting individuals. Furthermore, the longitudinal nature of the data is such that individuals are likely to have either changed address or possibly deceased since their last involvement with the criminal justice system during the specified study period. In addition, the personal identity of participants would be more difficult to preserve if the researcher was required to obtain consent as this would mean the researcher would require identified rather than de-identified data so that contact with participants could be made. Furthermore, to value add to offender recidivism databases and address gaps in information, it is often necessary to link data from separate sources and there are a number of impracticalities of obtaining consent in linkage-based population studies (see Holman, 2001). Scholars in the criminology field have also noted that there are many reasons why it may be desirable for offenders in a prisoner setting to agree to participate in a research project but it has been argued that asking for signed consent forms is often against the best interests of prisoners as signed consent forms create a record of participation in research and may pose threats to confidentiality (e.g., see Roberts & Indermaur, 2003, 2007-2008).

Thus, although waivers of consent must address all of the conditions specified in section 2.3.6 of the National Statement, it seems at least in the case of secondary research projects in the medical sciences and in criminology that the primary grounds for a waiver of consent are the impracticalities of obtaining consent, the need for representative/bias free samples, and the fact that confidentiality and anonymity may be compromised if consent was sought.

CONSENT WAIVER

In our case, the study involved two types of deceptions of participants:

1. Participants will not be aware that the website is constructed for research purposes and that certain aspects of their online behaviour will be recorded, namely whether they click on 'barely legal' and how they may respond to pop-up messages.

2. The study will mislead participants into believing:
   (a) that the fake web links actually lead to legal pornography; and
   (b) viewing 'barely legal' pornography may be illegal in some countries and attract a prison sentence.

These forms of deception are arguably at towards the beginning of the spectrum described by the National Statement (2.3). With respect to the social benefit that may arise from the study (2.3.1(b)), the study addresses an important and emerging social issue. Its objective is to inform the development of strategies to halter rapid expansion of the CEM market. This topic has vexed policy makers federally and draws considerable public consternation.

Importantly, the aims of the research could not be achieved if the aims of the research (or its method) are fully disclosed to participants. Clearly, if participants know that the links to pornography are fake, they are unlikely to click on them. Nor could the pop-up messages have any meaningful purpose if the participants knew they were generated for research purposes – and that the message about illegality was untrue. Likewise, informing participants about the research after their participation has ended could jeopardise the study. The fake website may need to operate for a number of months to achieve a suitable sample size. Once informed about the study, participants could distribute messages via the Internet that dissuaded others from visiting the site. In a worst case scenario the website could be hacked and disabled.

The study will involve low risks for the participants (2.3.1(c)). The study does not involve illegal acts. The identity of the participants will be difficult for third parties (or researchers) to establish in many case, and extremely difficult to establish in others. Other than slight inconvenience, some participants may experience mild distress if they are told that the 'barely legal' genre is

illegal, particularly if they have accessed this sort of pornography previously. This may lead some participants to check the laws in their country, or to alter their pornography viewing habits.

CONCLUSIONS

In this paper, we explored how it is feasible for HCI studies to be designed to monitor naïve participants without their consent whilst adhering to internationally recognised principles in research ethics. For the sake of scope, we have not discussed a) the challenges that researchers are facing when investigating CEM due to legal ramifications of even *pretending* to provide access to CEM and b) the challenges content providers would be facing when participating in such research. Cardinal issues for future projects seeking to seek HREC approval will be, among other things, demonstrating (a) beneficence (social benefit), (b) adequate protections for participant anonymity and (c) low risks of harms for participants.

ACKNOWLEDGMENTS

Participants, University of Tasmania REGS funding

REFERENCES

1. Allard, T. (2008). Child porn web broken by 70 arrests. *Sydney Morning Herald* 5/6/2008
2. Demetriou, C. & Silke, A. (2003). A criminological 'sting': experimental evidence of illegal and deviant visits to a website. *British Journal of Criminology*, 43, 213-222.
3. Dines, G. (2009). Childified women: How the mainstream porn industry sells child pornography to men. In S. Olfman (Ed.), *The sexualization of childhood,* Westport, CT: Praeger, 121-142.
4. Egelman, S., Cranor, L.F., Hong, J. (2008). You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. *Proc. CHI 2008*, Florence, Italy.
5. Niveau, G. (2010). Cyber-pedocriminality: Characteristics of a sample of Internet child pornography offenders. *Child Abuse & Neglect*, 34, 570-575.
6. O'Donnell, I. & Milner, C. (2007). *Child pornography: Crime, Computers and Society*. Cullompton, UK: Willan Publishing.
7. Prichard, J., Watters, P.A., & Spiranovic, C.A. (2011). Internet subcultures and pathways to the use of child pornography. *Computer Law & Security Review*, 27, 585-600.
8. Taylor, M. & Quayle, E. (2008). Criminogenic qualities of the Internet in the collection and distribution of abuse images of children. *The Irish Journal of Psychology.* 29(1), 119-130.
9. Williams, K. (2005). Facilitating safer choices: use of warnings to dissuade viewing of pornography on the Internet. *Child Abuse Review*, 14, 415-429.
11. Wortley, R 2012, 'Situational prevention of child abuse in the new technologies', in E Quayle & K Ribisl (eds), *Understanding and preventing online sexual exploitation of children*, Routledge, London, 188–204.
12. Wu, M., Miller, R.C., Garfinkel, S.L. (2006). Do Security Toolbars Actually Prevent Phishing Attacks? *Proc. CHI 2006*, Montréal, Québec, Canada.