serene risc Digest Volume 2, Issue 4

Cutting Edge Research Summaries for Policy-Makers and Practitioners

What is eWhoring?

eWhoring involves fraudulent behaviour. It is not only criminal, but also exploitative, through the deceitful use of images of (usually) young women.

Hutchings and Pastrana analysed 6,519 posts, written by 2,401 members, in 297 threads on a hacker forum to be able to understand the process by which this crime is generally committed. Those becoming involved in eWhoring start by learning from tutorials available online on hacking forum websites. Sources of difficulty for would be crimininals can be in the acquisition of images or video files, a demand which is met (and potentially fueled) by vendors on online forums. Analyzing the crime in stages provides insights into potential disruptions that could be introduced. This could include the promotion of distrust of tutorials, increasing the likelihood of image saturation, the verification of accounts, reducing the demand for images, and shutting down payment accounts, among others.

Do digital abusers lack self control ?

Young adults and adolescents have come to rely on the Internet in many aspects of their life, communications and forming relationships are not an exception. Marcus, Higgins, and Nicholson surveyed students from a mid-sized, American university to better understand the young people engaging in illicit behaviour on the web. It appears that frequent users of social networking, a large group in today's digital world, do not anticipate negative consequences from stalking behaviours. People with lower self-control were also less likely to foresee anger and rejection as a consequence of their cyberstalking activities.

What is a scambot and does it make money?

Mobile malware is a tactic used by cybercriminals to steal money from digital consumers. Fake dating apps with virtual (non-existant) prospective partners are among these apps. To gauge the extent of the fraudulent dating app ecosystem, Hu et al.'s systematic study puts forward a method for detecting these apps in Android mobile marketplaces. They identified fraudulent dating apps from a collection of more than 2.5 million apps downloaded from Google Play and nine unofficial Android stores. During their trials, male testers were eagerly contacted by various (seemingly) female service users. However, they were asked to pay a fee to be able to respond to these (fake) users. It is considered likely that fraudulent dating apps have made between 200 million and 2 billion US dollars in revenue.

Do Spyware vendors know what spyware is being used for?

Spyware tools have become readily accessible to the everyday consumer. An industry has been built on selling software enabling the monitoring of others. Harkin, Molnar, and Vowles looked into the marketing strategies employed in the spyware industry. Their analysis considered both visual and textual cues, considering not only explicit messages, but also implicit connotations. The advertising for applications generally suggested children, employees, intimate partners, and thieves as possible surveillance targets. Despite this, application vendors' terms and conditions provided contradictory disclaimers that placed all responsibility for illegitimate use on the client. The availability of consumer spyware and its clear potential for illegal and abusive use is troubling.

Does current cybersecurity models work for victims of intimate partner violence?

Our digital technology allows us to keep track of our whereabouts, conversations, schedules and more. The existence of powerful surveillance tools made available with blind trust has far-reaching implications for intimate partner violence, which is being made worse by abusers accessing their victims' digital lives. Freed et al.'s research identified the importance of digitally-enabled abuse in the context of intimate partner violence through a combination of individual and focus group interviews. The study uncovered four ways in which technology was exploited as a part of intimate partner violence. Intimate and family violence settings provides a unique security scenario that is difficult to manage with current technology and strategies. Current models of security struggle to deal with authenticated but adversarial users of a system.

What kinds of spyware are available?

Technology and software that provides knowledge of the movements, contacts, and personal information has become increasingly available. Chatterjee et al. systematically searched for spyware applications available online and on Google's Play Store. The intimate partner surveillance resources that were found included both free and paying apps. Only one of the uncovered tools was overtly described as spyware. Applications thinly veiled as legitimate that provide for the surveillance of intimate partner by non-technical repurposing appear to be readily available online.

Do Canadian women suffer from cyber-violence?

Women attending universities in Canada are at particular risk from cyber-sexual violence as they are both overrepresented as victims of sexual violence and keen users of technology. Cripps and Stermac's study surveyed female students at a university in Ontario. The survey participants comprised of eighty women from a sample of one hundred, all undergraduate students between the ages of 18 and 35. Participants we asked about their exposure to cyber-sexual violence and if they had reported or disclosed notable incidents. A majority of respondents admitted they had not disclosed instances of victimization. It appears that the experiences took a toll on the mental health of the participants. Cyber-sexual violence appears to have a real and significant impact on the those targeted.

Does technology feature in domestic violence cases?

New technologies have found their way into intimate relationships. Unfortunately, this also includes abusive relationships. Douglas, Harris, and Dragiewicz explored the role of technology in domestic and family violence by examining interviews with survivors of domestic abuse. 3% of women reported negative experiences involving these technologies. Harassment, monitoring, stalking, isolation (especially though constrained use), social-media-facilitated abuse, and image-based abuse were the among forms of behavior that were most discussed. Current understandings of intimate violence tend to focus on physical rather than digital forms of abuse. The facilitation of violence and coercive control through technological means is clearly an issue that justice and victim support services will have to understand in order to serve those affected by domestic and family violence.

Do teenagers suffer from digital intimate partner violence?

For better or worse, young people's abundant use of digital media now includes their love lives. Hellevik's exploratory study gauges adolescents' experiences with digital intimate partner violence and abuse. Interviews revealed four categories of digital partner victimization: humiliation, control, monitoring and sexual coercion. Victims suffered being the target of constant abusive calls and messages and the abusive use of social networks which could lead to the terrorisation of the victim.

Does the harm from cybercrime stop when the crime is reported?

Law enforcement often lacks the tools and expertise required to investigate and prosecute cybercrime. Cross investigated the experiences of online fraud victims with the criminal justice system. The study drew from a 2016 study with 80 Australian victims of cyber fraud. Fraud victims suffered from not knowing the role of different agencies, determining who to report to, reporting mechanisms being impractical and a lack of coordination between law enforcement leading to frustration. Leaving the jurisdictional mess of cybercrime investigation as "complex" appears to only harm victims and benefit criminals.

Understanding eWhoring

eWhoring involves fraudulent behaviour. It is not only criminal, but also exploitative, through the deceitful use of images of (usually) young women. eWhoring involves selling photos and videos with sexual content of another person to third parties. This is done by impersonating that person, real or not, in chat encounters to a third party, who pays for what they believe is an online sexual encounter.

Hutchings and Pastrana analysed 6,519 posts, written by 2,401 members, in 297 threads on a hacker forum to be able to understand the process by which this crime is generally committed.

Script analysis breaks a crime into a series of 9 steps from the preparation for the act to the after the act; namely preparation, entry , pre-condition, instrumentation pre-condition, instrumentation initiation, instrumentation actualization, doing, post-condition and exit.

Those becoming involved in eWhoring start by learning from tutorials available online on hacking forum websites. They then build a set of images both implicit to sell the veracity of their character and explicit to sell to a consumer. Next they create a character, complete with a backstory, alias and the accounts needed to engage with potential victims. They then create profiles in order to engage with consumers that make contact. A negotiation takes place to secure a price (for the transfer of images). After the payment is received the product is provided to the consumer. After the transaction the consumer is either discarded or maintained as a "good customer' and targeted with other ficticious personas or potentially with other scams.

Sources of difficulty for offenders in the commisssion of this crime can be in the acquisition of images or video files, a demand which is met (and potentially fueled) by vendors on online forums. Further issues are in the maintenance of accounts for characters, as platforms can ban characters involved in fraudulent activities. Proving that a fictitious character is real also presents problems, however this is often achieved by digitally faking 'proof of life' by superimposing text on images to show a requested date or name on an object within an image. Providing live 'cam shows' by dynamically stitching together prerecorded video can also be difficult to achieve realistically. Perhaps the greatest difficulty is in the processing and cashing out of payments to the character as payment platforms generally provide identity verification, which can be difficult for a person that does not exist.

Analyzing the crime in stages provides insights into potential disruptions that could be introduced. These could include the promotion of distrust of tutorials, increasing the likelihood of image saturation, the verification of accounts their use, reducing the demand for images, and shutting down payment accounts, among others.

The actors in this industry develop by mimicking and misappropriating the images of models for the purposes of commercial exchange with consumers. Besides the obvious defrauding of consumers this crime affects those models operating legitimate online sex businesses. Further, the criminals may misappropriate the images of those affected by personal account breaches. Innovation and evolution in this market such as the use of photorealistic simulations, chatbots and factual advertisement could convert this to a legitimate business. However, this alternative doesn't resolve issues relating to the objectification of women as portrayed by the virtual chatbots. eWhoring presents as an illegal industry built on cooperation between criminals and this may be in order to increase the market size and revenue of those selling image packs and crime tutorials. There are a number of potential reductive interventions each implementable at a different stage of the crime process.

eWhoring is a fraudulent practice that sells fictitious sexual encounters and can harm the customer, legitimate businesses, and creates a market for stolen intimate images.

Hutchings, A., & Pastrana, S. (2019). Understanding eWhoring. arXiv preprint arXiv:1905.04576.

Crossing Boundaries Online in Romantic Relationships: An Exploratory Study of The Perceptions of Impact on Partners by Cyberstalking Offenders

Young adults and adolescents have come to rely on the Internet in many aspects of their life, communications and forming relationships are not an exception. The intrusive level of access provided by technologies such as GPS and location tracking can become an 'electronic leash', and a means to violative, unlawful behaviour. Cyberstalking and cyber-harassment can be a recurring problem between romantically involved young adults.

Marcus, Higgins, and Nicholson surveyed students from a mid-sized, American university to better understand the young people engaging in illicit behaviour on the web. From a group of 500 thousand, 890 randomly chosen students completed a survey questionnaire. The survey was designed to assess the level of self-control of the participant, learn about the activities of their peers and record their perceptions of the possible consequences of cyberstalking behaviours. The resulting analysis showed support for the idea that those with lower self-control were less likely to foresee negative consequences, such as a break up, if their cyberstalking were discovered by a partner. Those that used social networking sites more frequently were less likely to think that partners would be angry about being cyberstalked. Younger people appeared to be less inclined to believe online harassment could harm their relationships. The results showed no clear link between the activities of peers and considering the effects of their actions, however there has been shown to be a link between self control and peers in other studies.

It appears that frequent users of social networking, a large group in today's digital world do not anticipate negative consequences from stalking behaviours. People with lower self-control were also less likely to foresee the anger and rejection as a consequence of their cyberstalking activities.

The emergence of the abuse of technology in intimate relationships is troubling, even though some perpetrators acknowledged this behavior would upset their partners, it still happens.

Marcum, C. D., Higgins, G. E., & Nicholson, J. (2018). Crossing boundaries online in romantic relationships: An exploratory study of the perceptions of impact on partners by cyberstalking offenders. Deviant Behavior, 39(6), 716-731.

Dating with Scambots: Understanding the Ecosystem of Fraudulent Dating Applications

Mobile malware can be used by cybercriminals to steal money from digital consumers. An example of this is fake dating apps with virtual (non-existant) prospective partners are among these apps. Through advertisements, messaging or subscription fees, these apps lure their users into giving away their money and data. Fraudulent dating apps make their users pay for premium services such as the ability to chat with (fake) female accounts. They seem to be an increasingly lucrative scam, but not much research has been done on this topic.

To gauge the extent of the fraudulent dating app ecosystem, Hu et al.'s systematic study puts forward a method for detecting these apps in Android's mobile marketplaces. The article presents a comprehensive analysis of the identified apps' developers, distributors, marketing gimmicks, profile accounts, and revenue.

They identified fraudulent dating apps from a collection of more than 2.5 million apps downloaded from Google Play and nine unofficial Android stores. They did this by first scanning the apps' names and descriptions were for eleven keywords in English and Chinese. Next, their programming code was inspected for a cash transaction component. The apps were then compared to find possible cloned apps from the same developer. Finally, a sample of apps were installed and tested.

Even though 3,697 individual apps were found, many had the same server address and digital fingerprint. A high proportion of their users' profiles were suspicious: fake users mostly shared the same 20 avatars. During their trials, male testers were eagerly contacted by various (seemingly) female service users. However, they were asked to pay a fee to be able to respond to these (fake) users. Once a conversation was started, the users' replies became incoherent. Apps stopped responding after the tester had paid for their 'premium' services.

The main way romantic fraud apps were promoted to smartphone users was via ranking fraud in the Android app stores. This is made possible by fake users who post favorable reviews and give five stars ratings that push these apps to the top of the ranking list. Another way fraudulent dating apps are promoted and distributed is through advertisement networks.

At the time of the study, 967 of these apps had 2,4 billion downloads. More than 44,000 negative reviews were collected, a number that could serve as a conservative estimate of the number of victims. Approximately between 1% and 10% of these apps' users ended up making payments. It is estimated that they spent on average between 5 and 15 US dollars per transaction. Consequently, it is considered likely that fraudulent dating apps made between 200 million and 2 billion US dollars in revenue.

Fraudulent dating apps are creating tens of thousands of victims, resulting in hundreds of millions of dollars lost.

Hu, Y., Wang, H., Zhou, Y., Guo, Y., Li, L., Luo, B., & Xu, F. (2019). Dating with scambots: Understanding the ecosystem of fraudulent dating applications. IEEE Transactions on Dependable and Secure Computing.

The commodification of mobile phone surveillance: An analysis of the consumer spyware industry

Spyware tools have become readily accessible to the everyday consumer. An industry has been built on selling software enabling the monitoring of others. To commercialize these products, vendors often portrait them as legitimate. However, this form of software is known to be used by controlling and abusive individuals in family and domestic violence situations.

Harkin, Molnar, and Vowles looked into the marketing strategies employed in the spyware industry. Their analysis considered both visual and textual cues, considering not only explicit messages, but also implicit connotations.

They studied the market to select a sample of nine spyware products. By searching the Web, the Apple Store and the Google Play store they identified the most popular (and likely, profitable) applications. In addition, a scan of Google Trends in Australia pointed to the most web-searched spyware tools. A template consisting of a series of descriptive and interpretative queries was used for the analysis of the nine resulting apps.

The advertising for applications generally suggested children, employees, intimate partners, and thieves as possible surveillance targets. To legitimize these apps, vendors relied on user recommendations and third-party endorsements. Almost all applications suggested using the software to target children and employees. A smaller proportion directly advertised the products use within intimate relationships. The software offered an operator the ability to surreptitiously monitor the activities, communications and location of their target; with some even providing the option of remotely sending 'spoof' SMS messages from a target device. Despite this, application vendors terms and conditions provided contradictory disclaimers that placed all responsibility for illegitimate use on the client. Unsurprisingly, the legal advice and customer support were primarily targeted at spyware operators, rather than their targets.

Despite the fine print of these applications disclaiming use outside of a context of two-party consent, their advertising makes their true purpose quite clear. The availability of consumer spyware and its clear potential for illegal and abusive use is troubling. Providing powerful surveillance tools under the guise of 'care' and 'security' commodifies malware for a general consumer audience. Although we are yet to fully understand the social impact of the security consumption, the potential for harm in abusive relationships is clear enough that concern is warranted.

Despite mandating their products be used legally, spyware operators are clearly aware of their harmful use to non-consensually spy on others.

Harkin, D., Molnar, A., & Vowles, E. (2019). The commodification of mobile phone surveillance: An analysis of the consumer spyware industry. Crime, Media, Culture, 1741659018820562.

"A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology

Our digital technology allows us to keep track of our whereabouts, conversations, schedules and more. This tracking is put in place in an atmosphere of trust; that the tracking is consensual, or that the monitor and monitored are one and the same. The existence of powerful surveillance tools made available with blind trust has far-reaching implications for intimate partner violence, which is being made worse by abusers' access to their victims' digital life.

Freed et al.'s research identified the importance of digitally-enabled abuse in the context of intimate partner violence through a combination of individual and focus group interviews. Discussions touched on the various ways technology was used by perpetrators to harass, control, and spy on their current or former partners.

The study was held in New York City. Both survivors and professionals were recruited with the help of the city's five Family Justice Centers; where social workers, therapists, attorneys, and prosecutors aid intimate partner violence victims. Eleven focus groups were held with thirty-nine survivors, and eighty-nine individual interviews were conducted with these survivors and fifty professionals.

The study uncovered four ways in which technology was exploited during intimate partner violence. Many victims had phones that were bought or paid-for by their abusers, allowing them to hold power over their monitoring features and use. Alternatively, easy-to-use, widely available spyware tools allowed culprits to compromise their partners' devices in order to monitor them. Some violent partners turned to text messages or social media posts to contact, harass, harm, threaten, and humiliate their targets and involve their friends and family. Finally, abusers violated the privacy of their victims and exposed them to risks, by posting their personal information or intimate images on the Internet.

Intimate and family violence settings provide a unique security scenario that is difficult to manage with current technology. Abusers may have formal ownership of the devices used by their victims, control their accounts and be inextricably enmeshed in their social networks. Current models of security struggle to deal with authenticated but adversarial users of a system. Digital technology provides additional mechanisms for monitoring that could contribute to enabling the coercive control of victims of intimate partner violence. Consideration for this security scenario and these victims should be incorporated into the design of software and victim support programs.

Intimate and family violence settings create a scenario where the device user is threatened by the device owner. Current security policies and technologies do not protect these victims.

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2018, April). ‚ÄúA Stalker's Paradise,‚Äù: How Intimate Partner Abusers Exploit Technology. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (p. 667). ACM.

The Spyware Used in Intimate Partner Violence

Technology and software that provides knowledge of the movements, contacts, and personal information has become increasingly available. This may be spyware, designed to specifically to monitor others, or generally benign monitoring applications misappropriated for such a use. Such tools and applications create additional risks in intimate partner violence situations as they can provide powerful features to abusers seeking to control and intimidate.

Chatterjee et al. systematically searched for spyware applications on Google search and Google Play store. Their analysis assessed the scope of surveillance tools available to abusers. They also sought to better understand the strategies of vendors and the range of available anti-spyware resources.

Through manual and automated techniques, both Google's web engine and app store were crawled in search of intimate partner surveillance tools. Using manual review, machine-learning, and an algorithmic search, the results were scanned for spyware tools. Seventy of the resulting apps were then manually analysed in order to uncover their design and capabilities. They also assessed the developer's role in the illegal or abusive use of their products, by investigating user comments, advertising, and customer support.

The intimate partner surveillance resources that were found included both free and payed apps. Based on their intended uses, the individually reviewed apps were categorized into three groups: (1) personal tracking apps, which are designed for a sole phone owner to monitor their device or self; (2) mutual tracking apps, intended for two or more people to be able to track each other's devices; and (3) subordinate hacking tools allowing unilateral tracking or monitoring of a targeted device, without a need for their consent.

None of the uncovered tools were overtly described as spyware. Some of the app could be decribed as dual use, meaning they had an official, intended purpose that could nevertheless be subverted by an abuser. Oftentimes, these apps underlined their legitimate intent on the official store, yet advertised illegitimate usages elsewhere. By knowingly encouraging the illicit misuse of their products, some developers could thus be described as tacitly facilitating intimate partner surveillance.

Applications thinly veiled as legitimate that provide for the surveillance of intimate partner by non-technical repurposing appear to be readily available online. These applications represent a source of potential harm for victims of intimate partner violence.

Spyware applications that can be used to abuse others are easily available to non-technical users.

Chatterjee, R., Doerfler, P., Orgad, H., Havron, S., Palmer, J., Freed, D., ... & Ristenpart, T. (2018, May). The spyware used in intimate partner violence. In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 441-458). IEEE.

Cyber-Sexual Violence and Negative Emotional States among Women in a Canadian University

Women attending universities in Canada are at particular risk from cyber-sexual violence as they are both overrepresented as victims of sexual violence and are keen users of technology. Cyber-sexual violence can include a range of activities including sexual harassment, the threat or practice of creating or distributing of intimate or sexual assault images of a person, or even the arrangement of an assault; all of which are considered as harmful sexually aggressive behaviours assisted by technology.

Cripps and Stermac's study surveyed female students at a university in Ontario. They assessed the students' experiences with cyber-sexual violence, as well as the rates at which they reported them to the authorities. They also hoped to uncover the effects of this violence on its victims' emotional states.

The survey's participants comprised of eighty women from a sample of one hundred, all undergraduate students between the ages of 18 and 35. Participants were asked about their exposure to cyber-sexual violence and if they had reported or disclosed notable incidents. The emotional states of the participants were also recorded.

The occurrences of cyber-sexual violence reported by the students varied. Online forms of gender-based hate speech and sexual harassment were more common than non-consensual porn and rape-related offenses. A majority of respondents admitted to instances of victimization that they had not disclosed.

It appears that the experiences took a toll on the mental health of the participants. Having been the target of the aforementioned abusive behaviors was linked to depression, anxiety, stress and, to the greatest extent, post-traumatic stress. These symptoms occurred regardless of whether a victim had shared her experience or not.

Cyber-sexual violence appears to have a real and significant impact on the those targeted. As evinced by the experience of women within universities in Canada, the incorporation of technology into modern lifestyles may have increased the risk to women of this form of violence.

Women at Candian universities suffer from being targets of cyber-violence, however the majority of them do not report it.

Cripps, J., & Stermac, L. (2018). Cyber-Sexual Violence and Negative Emotional States among Women in a Canadian University. International Journal of Cyber Criminology.

Technology-Facilitated Domestic and Family Violence

New technologies have found their way into intimate relationships. Unfortunately, this also includes abusive relationships. Victims of Domestic and Family violence have attested to the digital dimension of abuse now made possible. The term 'coercive control' describes those patterns and behaviors by which an abuser controls their partner. In the context of intimate abuse, technology is often a means to coercive control.

Douglas, Harris, and Dragiewicz explored the role of technology in domestic and family violence by examining interviews with survivors of domestic abuse. In examining interviews collected from sixty-five women between 2014 and 2017, the subjects were asked to recall instances of domestic and family abuse. Even though they were not explicitly asked about technology-facilitated violence, survivors identified instances in which connected devices, communication networks, and digital media were used as a means of coercive control.

Eighty-three percent of women reported negative experiences involving these technologies. Harassment, monitoring, stalking, isolation (especially though constrained use), social-media-facilitated abuse, and image-based abuse were the forms of violent behavior that were most discussed. Women's recollections involved more than one type of technology. Even though smartphones were overwhelmingly cited, computers, texting, cameras, recording devices, software, and online accounts were also mentioned. Technology was used to monitor the activities, whereabouts and communications of a partner allowing the abuser to invade the private spaces of their victim or confront them post-separation. Alarmingly, the children of victims were also sometime involved as unwitting participants.

Current understandings of intimate violence tend to focus on the physical rather than digital forms of abuse. The facilitation of violence and coercive control through technological means is clearly an issue that justice and victim support services will have to understand in order to serve those affected by domestic and family violence.

Digital forms of abuse have become a part of intimate partner violence. Support services should be aware and equipped to deal with technology-facilitated domestic violence.

Douglas, H., Harris, B. A., & Dragiewicz, M. (2019). Technology-facilitated domestic and family violence: Women's experiences. The British Journal of Criminology, 59(3), 551-570.

Teenagers' personal accounts of experiences with digital intimate partner violence and abuse

For better or worse, young people's abundant use of digital media also includes in their love lives. Digital partner violence opens the door to new forms of abuse, such as monitoring and cyber harassment, while exacerbating pre-existing problematic behaviours, such as stalking and harassment.

Hellevik's exploratory study gauges adolescents' experiences with digital intimate partner violence and abuse. Interviews were analysed to assess how technology-facilitated abuse affected participants, and how it related to other forms of dating violence.

Transcripts were retrieved from "Safeguarding Teenage Intimate Relationships", a study of the European Union held in five countries. Twenty-one of the one hundred interviewed participants were from Norway. This study's sample is the forteen Norwegian subjects who declared having suffered digital partner abuse. Aged from fifteen to eighteen; including twelve females and two males. Interviews were thematically analysed to classify the subjects' experiences. This revealed four categories of digital partner victimization, harrassment, control, monitoring and sexual coercion. Harassment often took the form of humiliation, barraging, scaring, and berating of the victim. Control was exerted by restricting their social contacts, social media expression, and general autonomy. Monitoring aimed to gain knowledge of a partner's whereabouts, contacts, and activities. Sexual coercion was the pressuring, humiliation, or threatening of a victim to gain favors, threaten sexual violence, or non-consensually distribute intimate images.

Victims related suffering from being the target of constant abusive calls and messages. In some cases text messages enhanced the severity of the harassment, perhaps due to lack of emotional cues in text or the victim re-reading abusive messages on their phone. Abusive partners would also involve the victim's social network in the abuse, both to make public private abuses and as a form of surveillance or by taking control of their accounts, deleting posts/comments, blocking users, etc. This impacted the victim's behavior as they became terrified that friends would innocently mention or tag them in a photo or a post, revealing their activities to the abuser.

Teenagers are not immune from the digital aspects of intimate partner violence, suffering abusein the forms of harassment, control, monitoring and sexual coercion.

Hellevik, P. M. (2019). Teenagers' personal accounts of experiences with digital intimate partner violence and abuse. Computers in Human Behavior, 92, 178-187.

"Oh we can't actually do anything about that": The problematic nature of jurisdiction for online fraud victims

Crime has changed, and law enforcement often lacks the means necessary to adequately investigate and prosecute cybercrime. Moreover, since traditional legal frameworks are based on territoriality and state jurisdiction, a significant portion of online crime, which very often involves more than one country, go unresolved. As a result, victims' experiences with the police can be frustrating and inconclusive.

Cross investigated the experiences of online fraud victims with the criminal justice system. Interviews aimed to unveil their views on cybercrime jurisdiction. She analysed these interview hoping to discover any misconceptions surrounding the policing of their case, as well as the challenges arising from the international nature of their ordeals.

The study drew from a 2016 study with eighty Australian victims of cyber fraud; victims of crimes ranging from romance fraud to investment fraud. From of this larger study, twenty-six of the participants mentioned the police in their interviews, permitting a greater understanding of their views.

The participants recollections about dealing with jurisdictional issues could be distilled into four major points:

- Victims were often confused about different agencies' role and authority. There is a misconception that international crime is reported to the federal police force, whereas individual cases should be reported to local police. Alarmingly, some local police appeared to share this misconception.
- Barriers imposed by jurisdiction pertained not only to international crime, but also to the national structure of law enforcement, Australia having differing legislatures and justice systems in each state. Victims often faced difficulties in determining which police to report the crime to.
- Reporting cybercrime involved considerable practical challenges. Procedures for criminal complaints may involve a requirement for reporting the crime in person, which is particularly problematic for international crimes.
- Complaints were hampered by lacking coordination between law enforcement. Instances where law enforcement overseas were willing to investigate but required local police to coordinate with federal police to open and refer the complaint resulted in frustration due to domestic unresponsiveness.

Dysfunctional approaches to the issue of cross border crimes can exacerbate the harms suffered by the victims of cybercrime. Awareness of how cross jurisdictional crimes are to be reported and subsequently handles would benefit victims of cybercrime. Transparency on the handling of crimes reported to online platforms would also be beneficial. Leaving the jurisdictional mess of cybercrime investigation as 'complex' appears to only harm victims and benefit criminals.

The complex jurisdictional issues of cybercrime leave victims frustrated in their attempts to engage with law enforcement. The current state harms victims and aids criminals.

Cross, C. (2019). "Oh we can't actually do anything about that": The problematic nature of jurisdiction for online fraud victims. Criminology & Criminal Justice, 1748895819835910.

serene-risc.ca

Smart Cybersecurity Network (SERENE-RISC) is a knowledge mobilization network that aims to be a cybersecurity exchange that is recognized as an open, inclusive, and unbiased forum to unlock the value of knowledge on cybersecurity risks, threats and solution for all Canadians. We are a network of networks that provides publications, tools, events, professional development and education. We are always looking for partners to collaborate to make cybersecurity better, so please contact us to find out more.

konnect.serene-risc.ca

We are building the Canadian source for summaries of research, opinion pieces, video presentations, fraud bulletins, public awareness materials and more. You can filter the collection by type of content, click on keywords or search. The website provides lots of original conent produced by us and in collaboration with partners. To save your time, ee are sending an email regularly a summary of the new content to save you time and make it easier to find content. You can subscribe to this list online at: **http://konnect.serene-risc.ca/subscribe-abonnement/**

We will be looking for contributions to this page from our community, so if you have an idea for a piece that you would like to share please let us know.

You can help by:

- Subscribing to the regular update online at: **http://konnect.serene-risc.ca/subscribe-abonnement**
- Following **@SERENE_RISC** on twitter and retweeting,
- Joining the Linkedin Group and submitting or commenting on posts, and
- Posting links to **konnect.serene-risc.ca** content on other platforms you are involved with.

cybersec101.ca

Want to provide basic cybersecurity classes but don't know how or have the time to get started?

We have developed evidence-based materials that can help you quickly put on training programs. Find resource sheets, presentation videos, class tools and slides to build basic cybersecurity education and awareness sessions at. There are ten modules in French and English with materials to help from basic concepts to practical step-by-steps for better security online.

donate

We are now accepting donations to help us provide more services that are open, accessible, inclusive and ubiased. You can download a donation form at https://www.serene-risc.ca/donation or contact us for more information at info@serene-risc.ca

 @SERENE_RISC  /serenerisc  /serene-risc

The SERENE-RISC Cybersecurity Knowledge Digest

Editor-in-Chief: Michael Joyce
Scientific Editor: Benoît Dupont
Editors: Marco Mendoza

Government of Canada Gouvernement du Canada
Networks of Centres of Excellence Réseaux de centres d'excellence

serene risc

Université de Montréal