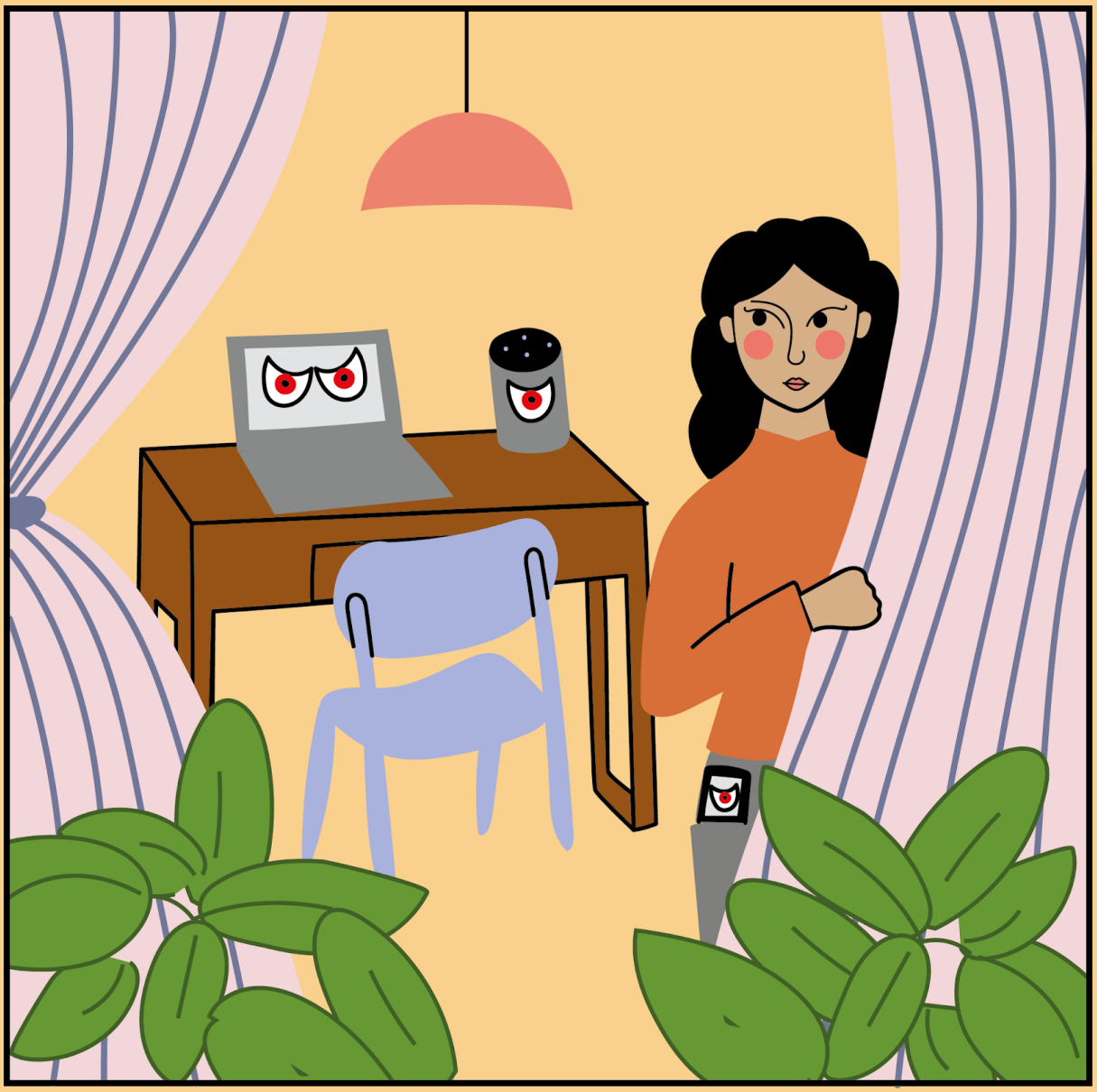
MAPPING THE STATE OF KNOWLEDGE ON THE USE OF STALKERWARE



IN INTIMATE PARTNER VIOLENCE

Tomás Bermudez*, Maddalena Esposito* and Jay Neuner*

London, September 2020

© Tomás Bermudez, Maddalena Esposito, and Jay Neuner

A dissertation submitted to the faculty at University College London in partial fulfilment of the Master of Public Administration degree in the Department of Science, Technology, Engineering & Public Policy.

*All authors contributed equally to this work and consider it a collective creation

© Tomás Bermudez, Maddalena Esposito, and Jay Neuner

ALL RIGHTS RESERVED

Abstract

Through a multi-disciplinary approach, this research profiles the state of knowledge on the use of stalkerware in intimate partner violence. Exploring past research and current, direct assessments from experts, it identifies key terms and descriptions associated with stalkerware, as well as gaps in current research on the subject. Researchers across academia, the voluntary sector, the statutory sector, and the private sector illuminate their experiences and perspectives on knowledge about stalkerware use in intimate partner violence, contributing to an overview of the knowns and unknowns in addressing this issue. These insights reveal the need for increased and cross-sectoral knowledge development, from the statistical (such as data on the prevalence of the issue of stalkerware use in intimate partner violence) to the sociological (notably, the experiences of victims and survivors). Through this research, stakeholders across sectors can prioritise future research and actions to address this issue.

Acknowledgements

We would like to thank Dr Leonie Tanczer (UCL STEaPP) for her academic assistance, as well as Hera Hussain (Chayn). We are further grateful to the staff and faculty of UCL STEaPP for their assistance and support. We also thank the participants who were involved in this project and attendees of the 2020 'Hackers on Planet Earth' (HOPE) conference.

TABLE OF CONTENTS

Abstract 1
Acknowledgements 1
TABLE OF CONTENTS 2
Boxes, Figures and Tables 4
Introduction 5
Recommendations for Policy Makers 5
The Present Research 8
Study 1. Literature Review 9
Methods 9
Results 11
Discussion 16
Study 2. Interviews 18
Methods 18
Results 20
Discussion 24
Study 3. Survey 25
Methods 25
Results 26
Discussion 31
Limitations and Challenges 33
Overall Discussion 34
Current and Future Knowledge 34
Culture as a Defining Factor 35
Potential Solutions and Existing Hurdles to Legislative Approaches 36
Next Steps 38
Conclusion 39
References 40
Appendix B. High-Relevance Texts from Literature Review 43
Appendix C. Coding for Literature Review 45
Appendix D. Interview Questions 46
Appendix E. Survey Questions 49

Boxes, Figures and Tables

List of Boxes

Box 1. Notable high-relevance texts 14

List of Figures

Figure 1. Number of publications by topic of focus from 6 May 2010 to 5 May 2020 12
Figure 2. Terms used to reference technology that enables stalking, harassing and related actions 13
Figure 3. Frequency of terms used in reference to stalkerware use in IPV 25
Figure 4. Categorisations of stalkerware 26
Figure 5. Categorisations of stalkerware (continued) 26
Figure 6. Characteristics of stalkerware 27
Figure 7. Concerns about risks associated with stalkerware 28

List of Tables

Table 1. Search terms from ProQuest query string, 5 May 2020 9
Table 2. Example of theme and sub-theme development in interview coding 18

INTRODUCTION

Intimate partner violence (IPV) is often a fast-evolving situation, rife with risk. So, too, is technological development, and the intersection of these two phenomena has resulted in a disturbing, fast-moving, high-risk new reality: technology-facilitated abuse.

Technology-facilitated abuse, or 'tech abuse', describes the use of social media, devices, software, and other technologies to monitor, harass, stalk, and abuse intimate partners (as well as former partners and other targets). These actions can range widely – from verbal abuse via direct text messages, to image-based abuse, to defamatory social media postings, to forcing a partner to share a device password, to physically tracking a victim.

One category of technologies that has emerged in research and discussion about this issue is 'stalkerware', also commonly referred to as 'spyware.' Our working definition of stalkerware as we began this research was 'technologies used to "stalk" or spy on others' activities via their "infected devices"'. Examples include mobile applications available on publicly accessible app stores, such as mSpy on Google Play, but also include unnamed software available through direct liaison with developers.

Yet the definition shared above is only one; as an initial review of the literature revealed, stalkerware is an incredibly complex topic with little consensus among experts as to what its founding features are. Notably, most discussion of tech-facilitated abuse has focused on other technologies, such as social media, while discussion of spyware has most often focused on technologies used in the context of state-based surveillance. The topic of stalkerware in IPV, instead, has been covered sparingly and only in specific regional contexts. Thus, we set out to map the current state of knowledge on stalkerware use in IPV.

We first identified critical gaps in the current research. These included:

- a commonly shared definition of 'stalkerware', notably consensus on what technology or technologies constitute stalkerware and their key features;
- who is conducting research, and where;
- the hurdles to knowledge gathering in this field; and
- how existing and future knowledge can best enable different stakeholder groups to act upon this issue.

Through our research, we aimed to fill as many of these gaps as possible, as well as provide critical context to help others fill these gaps in future. In this way, we support increased knowledge development and sharing to help shape how academia, the voluntary sector, the statutory sector and media discuss and address the issue of stalkerware use in IPV.

RECOMMENDATIONS FOR POLICY MAKERS

While we believe this research can support efforts across sectors, it has revealed a particularly valuable set of insights to inform both current understanding and future pathways in the realm of policy making.

Recommendation 1: Multi-stakeholder Learning and Research Development

To further develop knowledge among all sectors and stakeholders critical to this work, policy makers have the opportunity to lead multi-stakeholder learning and research and development across academia, the tech sector, the voluntary sector, and the statutory sector. Specifically, such engagement should consist of co-developed research and knowledge transfer on:

- shared definitions of stalkerware and technologies used to perpetrate harms like stalkerware (such as the work undertaken by the Coalition Against Stalkerware);
- the technical contexts of stalkerware's implementation, including how it can be detected and the most effective means of safely disabling or removing it (such as the work of the Clinic to End Tech Abuse in New York City); and
- the experiences and needs of victims/survivors, particularly with regards to ensuring their safety.

Recommendation 2: Funding Further Research

Subsequently, policymakers should allocate funding to research on stalkerware use in IPV. Research funding should be allocated in the form of grants from national scientific bodies, in-house research development or external consultations across academia, the tech sector, the voluntary and the statutory sector.

A similar initiative was put forward by the Australian Communications Consumer Action Network (ACCAN), a peak body representing communication consumers' rights. ACCAN provided a research grant for Deakin University's research into consumer spyware in 2019 (Molnar & Harkin, 2019); the work of ACCAN is in turn provided by the Commonwealth of Australia through Article 593 (2) of the Telecommunications Act of 1997 (Australian Government, 2017). Similarly, the broader work of the IPV Tech Research at Cornell and NYU was funded by grants from the National Science Foundation (Computer Security and Privacy for Survivors of Intimate Partner Violence, n. d.).

Funds should be allocated to multidisciplinary efforts, specifically to explore the following:

- data on the prevalence of stalkerware use in IPV;
- on-device detection solutions for stalkerware;
- experiences of victims/survivors of stalkerware abuse.

Recommendation 3: Multi-stakeholder Review of Legislation

Given the fragmented legislative frameworks governing the malicious use of stalkerware, policymakers should engage in multi-stakeholder review of legislation. As emerged from our studies, stalkerware use is a cross-jurisdiction issue; moreover, in some geographical contexts there may be existing laws that cover its malicious use, while in others stalkerware abuse might be unaddressed. Reviews of legislation should engage consultations with stakeholders from a range of backgrounds and should be conducted to:

- assess the current legal framework(s) governing the use of stalkerware technologies in IPV;
- consider the update of existing legislation to include technology-facilitated abuse; or
- consider the creation of legislation on the use of stalkerware technologies in IPV.

These three processes should be an iterative endeavour, should be conducted cyclically for legislation and regulation to be up to date with technological advancements.

A similar endeavour was conducted in 2012 in the UK with the *Review of the Protection From Harassment Act 1997*. The UK government launched a targeted two-month consultation to inform a decision as to whether the Act and other legislation provided adequate legal protection to victims of stalking and if there should be a specific criminal 'stalking' offence in legislation (UK Home Office, 2012). The consultation invited the views of key stakeholders working on or affected by stalking, including the police services, government departments and voluntary sector organisations (UK Home Office, 2012).

Recommendation 4: Funding to Frontline Services

Beyond research and knowledge sharing and multi-stakeholder engagement, policy makers should also prioritise funding to increase frontline services' resources as they provide direct support to victims and survivors. Police services, as part of frontline services, should require additional resources to tackle stalkerware abuse, too. However, considering law enforcement's ability and capacity to appropriately handle incidents of IPV, cross-disciplinary knowledge and awareness raising is urgently needed, particularly from support services on the care and wellbeing of victims/survivors.

A government initiative that improved training and awareness raising within the voluntary and statutory sectors is the Australian eSafety Commissioner, a government agency that deals with citizens' online safety. Through its eSafety Women division, it provides specific technology-facilitated gender-based violence training to frontline workers and specifically to social and support workers, mental health workers, legal workers, police, and to government and academia (Australian Government eSafety Commissioner, 2020a). Further, the Commissioner established an Online Safety Grants Programme, a grant funding of 9 million AUD for the voluntary sector to deliver online safety education and training for children and the general population (Australian Government eSafety Commissioner, 2020b).

Based on the present research, funding to support organisations and law enforcement should be allocated to:

- Increase awareness of the potential use of stalkerware use in IPV;
- Improve training on how to best ensure the safety of victims, survivors, dependents, and others at risk due to physical or emotional proximity; and
- Expand capacity to detect stalkerware and to deal with stalkerware abuse.

Conclusions

Through these efforts, policy makers can help handle the most urgent challenges in this field first and foremost. These initiatives can also ensure the future trajectory of this phenomenon provides systemic change across the relevant sectors, including academia, the technology sector, law enforcement, support services, and its own.

THE PRESENT RESEARCH

Through initial research we found that the knowledge on stalkerware was fragmented – terminology and definitions lacked consensus, and current research on the topic was limited to specific regional contexts, whilst being a fast-evolving and growing transnational issue. Without foundational context, future knowledge and interventions on this issue will lack structure and focus to address stalkerware use in IPV and its effects.

Our research primarily aims to set the parameters for those foundations, guiding future research and action in the field. The project was carried out in partnership with Chayn, a global volunteer network addressing gender-based violence, to assist their work in this regard. We believe, moreover, that this research will aid a broader range of organisations within the voluntary sector, as well as private companies, government bodies, and others working on behalf of victims and survivors, in doing the same.

We modelled our research after Lee Jarvis and Stuart Macdonald's study *What Is Cyberterrorism? Findings from a Survey of Researchers* (2014), which employed a survey of researchers to gauge the global research community working on and around cyber terrorism. Jarvis's and Macdonald's objective was to gather expert views on the term 'cyber terrorism', to understand how and if ambiguous terminology affected research and policy, and, ultimately, to assess the current state of the research field and highlight any research gaps.

In our preliminary research we found that the research field on cyber terrorism and on stalkerware shared key features; they were, or are, both nascent fields dealing with a complex, evolving area of technology use, and both are transnational in nature. Another similarity between the two studies was the fragmented nature of the research field. Additionally, the terminology and definitions for both concepts at the time of study were contested. Considering these similarities, we decided to design our project after Jarvis's and Macdonald's work.

Our research consists of three interdependent studies that attempt to take stock of the knowledge base in this field through multiple modes and perspectives.

STUDY 1 is a literature review of research publications published between May 2010 and May 2020. Through this review, we mapped key characteristics of past research to date and we noted research trends over time to understand the evolution of the field.

STUDY 2 is a set of 23 semi-structured interviews carried out with key researchers working in or with experience in the field of stalkerware and intimate partner violence. In this study we focused on researchers' experiences and approaches, as well as their understanding of critical terms and issues. In conjunction with Studies 1 and 3, this allowed us to assess not just the present state of research, but its pathways for growth.

STUDY 3 is a survey of researchers conducted from late July to early August 2020. Through this study we intended to qualify observations obtained from the interviews and stress-test them over a large pool of respondents.

The goal of the three studies is to highlight intersecting and differing insights on the subject. Ultimately, our focus was the same as that of Jarvis and Macdonald. How is stalkerware defined? What encompasses stalkerware? What are the challenges to understanding stalkerware use and its effects, as well as to acting upon it?

This paper proceeds in five stages. The three studies will be discussed in sequential order. Subsequently, the paper will discuss the limitations and challenges to our approaches and findings. Lastly, the paper will provide an overall discussion of the three studies.

STUDY 1. LITERATURE REVIEW

Study 1 is a comprehensive literature review that looked to gather data on the existing publications addressing stalkerware. The aim of Study 1 is to assess the state of current research on stalkerware and IPV, and to highlight key concerns and gaps present in the literature published thus far, while also mapping aspects of a list of relevant publications.

The insights gained from Study 1 also served to inform the interview questions in Study 2 and to guide our participant outreach for Studies 2 and 3.

Methods

The method underpinning Study 1 was modelled after a systematic literature review, with alterations made to address the constraints of the project. A systematic literature review (SLR) is a method that aims to form an evidence-base into a topic to advance policy and research (Boell & Cecez-Kecmanovic, 2015). The distinctive feature of an SLR is a protocol that prescribes how to 'identify, select, assess and synthesise evidence from the literature' (Boell & Cecez-Kecmanovic, 2015) in an iterative, consistent and systematic way through a database (Khan et al., 2003). SLRs are usually conducted over a timeframe that spans between two and eight months and are conducted in a team to enable researcher triangulation (Grant & Booth, 2009).

Of the SLR method, our approach applied researcher triangulation, the use of a search, coding and analysis protocol, and researcher triangulation. However, it departed fundamentally from the SLR method in that some of the literature analysed was obtained informally through desk research and through the suggestions of our supervisor, Dr Leonie Tanczer. Moreover, our review was completed in just two months, as opposed to the longer timeframe of the SLR approach. These adjustments were made to address the resource and time constraints of our research team and of our project.

Initial Informal Search

The foundation of our literature review was an informal search of publications on stalkerware and IPV which provided initial knowledge on stalkerware and on its intersection with IPV. This first body of literature amounted to 17 texts that helped us develop relevant keywords, as well as inclusion and exclusion criteria, for our formal search.

Structured Search: Inclusion and Exclusion Criteria

The structured searches consisted of iterative searches using a list of keywords and Boolean operators through the multi-disciplinary database ProQuest (Table 1). Other databases such as Scopus and Google Scholar were found inadequate for the scope of our project, as the former only focused on academic publications and the latter did not provide satisfactory mechanisms to apply a structured search using Boolean operators. Our search included publications from a range of actors, namely academia, news media, advocacy organisations, government, the private sector, and independent researchers. During the literature coding phase, we also decided to exclude all press releases from our final sample pool. Due to the joint language abilities of our team, we limited our search to English-language texts.

Final ProQuest Query String
Group 1: (stalkerware OR spyware OR spouseware OR creepware OR "dual*use" OR "parent* control app*" OR "anti-virus" OR "malware")
Group 2: AND (domestic violence" OR "intimate partner violence" OR "gender*based violence" OR "domestic abuse" OR "tech*?facilitated abuse" OR "partner abuse" OR "tech* abuse" OR "online abuse" OR "family violence" OR "abusive relationship" OR "controlling relationship")

Table 1. Search terms from ProQuest query string, 5 May 2020

Each iteration intended to improve the overall relevance of texts. We selected texts that had a direct mention of stalkerware technology and IPV, though with differing terminology. We excluded publications that did not explicitly refer to stalkerware used in IPV or did not discuss applications or software used in those contexts with the functions commonly associated with stalkerware or spyware, as identified from the initial, informal literature review.

Final Search

We carried out our final search through ProQuest on 5 May 2020. Our final search yielded 1,613 total publications published between 2010 and 2020. This was a sufficiently large pool of results with a high proportion of relevant texts relative to our other searches. Importantly, it included all key texts from our informal literature review.

We reviewed the first 1,200 results and, based on our inclusion and exclusion criteria, selected 228 relevant publications. This included 30 high-relevance publications (Appendix B). These publications were then coded to allow for general quantified observations of aspects of the literature. The literature coding referred to the topic of focus, research methods, type of publication and relevance (Appendix C).

Relevance was assessed on three levels: high, medium and low. The intention was to streamline texts that fit our research questions and highlight key publications. High-relevance texts included publications that were completely focused on

the issue of stalkerware and IPV with active research into different aspects of the issue, including the functions of stalkerware, the marketing of stalkerware, detection and classification of stalkerware. Medium-relevance texts referenced stalkerware multiple times and produced new knowledge related to the subject but either discussed existing research or did not focus primarily on stalkerware. Low-relevance texts contained some mention to stalkerware and IPV, but either did not delve deeply into the issue or dealt with it as a part of a broader topic, such as technology-facilitated abuse.

Results

Chronology and Region

Out of 228 total sources, we coded 30 high-relevance texts, 73 medium-relevance texts, and 125 low-relevance texts. High-relevance publications were spread largely amongst the United States (30%, or nine publications), United Kingdom (16.6%) and Australia (13.3%) with the second-highest group being trans-nationally focused (i.e. explicitly covering a global scope, rather than one specific region) (20%). South Africa, Canada, Brazil and India were also countries of focus for several high-relevance texts. These distributions were also likely influenced by the English language restriction of the search.

Among our selected literature, early publications (from 2010) were primarily published in the UK and US, alongside a Canadian and Irish publication. The number of publications in the US grew, spiking in 2014 (14) with smaller peaks in 2017 (10) and 2019 (9). The number of publications in the UK grew more steadily, reaching 10 in 2018 and 11 in 2019. It took until 2012 for Australia to produce a publication on stalkerware, with subsequent publication numbers spiking in 2017 (13) and 2019 (21). The number of publications in Australia in 2019 is the highest number in one year in any country. 2019 is to date the year with the most publications in one year, among those studied, at 56 publications. 47.1% of academic publications (academic journals, academic research publications and PhD dissertations) are focused on the US, with the second highest geographical focus being trans-national publications.

Source Types, Methods and Topics

With regards to the source type, academic publications (34 publications, totalling 14.9% of all publications) have the widest variety in methods (14) while other source types have publications covering two to three methodologies. The most used methodologies across these publications were legal analysis (11), technical studies (9), surveys (9) and literature reviews (8). It is also worth noting that research methods focused on language analysis – semiological (1 publication), content (3) and discourse analysis (5) – which were used in nine instances. Methods that required direct interaction – specifically participant observation (1) and interviews (4) – were used in 5 publications.

In terms of topics, a significant share of the academic publications focused primarily on tech-facilitated abuse (34.8%, 11 publications) and on stalkerware (14.5%) with detailed delving into both topics. All PhD dissertations focused on tech-facilitated abuse. This could indicate an increased interest in tech-facilitated abuse in academia and follows the growing trend in the literature, as noted above. 50% of trade media publications, of a total of 18, either dealt with tech-facilitated abuse or mentioned stalkerware generically. Within trade media, 33.3% of publications focused on the legal challenges posed by stalkerware.

From the total 228 results, 69.7% were published in news media outlets. Key news media texts included a publication from *The Times* (UK) published on the availability of stalkerware through Google platforms and the need for urgent action, which also included interviews with police management and a case study on a specific incident of stalkerware use (Bridge et al., 2018). 30.8% of news media publications followed the same structure of analysis upheld by interviews with survivors, front-line workers, academics, or police amongst other groups.

The number of publications by topic fluctuated yearly as seen in Figure 1. The data shows consistently growing interest in publications on tech-facilitated abuse throughout the observed ten-year period, and notably a significant spike in interest on stalkerware in 2019 as compared to past years. 2015 and 2016 saw the highest number of publications on the legal challenges related to stalkerware in one year (six publications) while 2017 and 2019 each saw the publication of five sources focused on the experiences of survivors of tech abuse respectively. 2019 is the year with most publications and the year with the most publications on anti-stalkerware practices thus far, with the caveat that literature selected for 2010 and 2020 covered partial years (post-6 May 2010 and pre-5 May 2020).

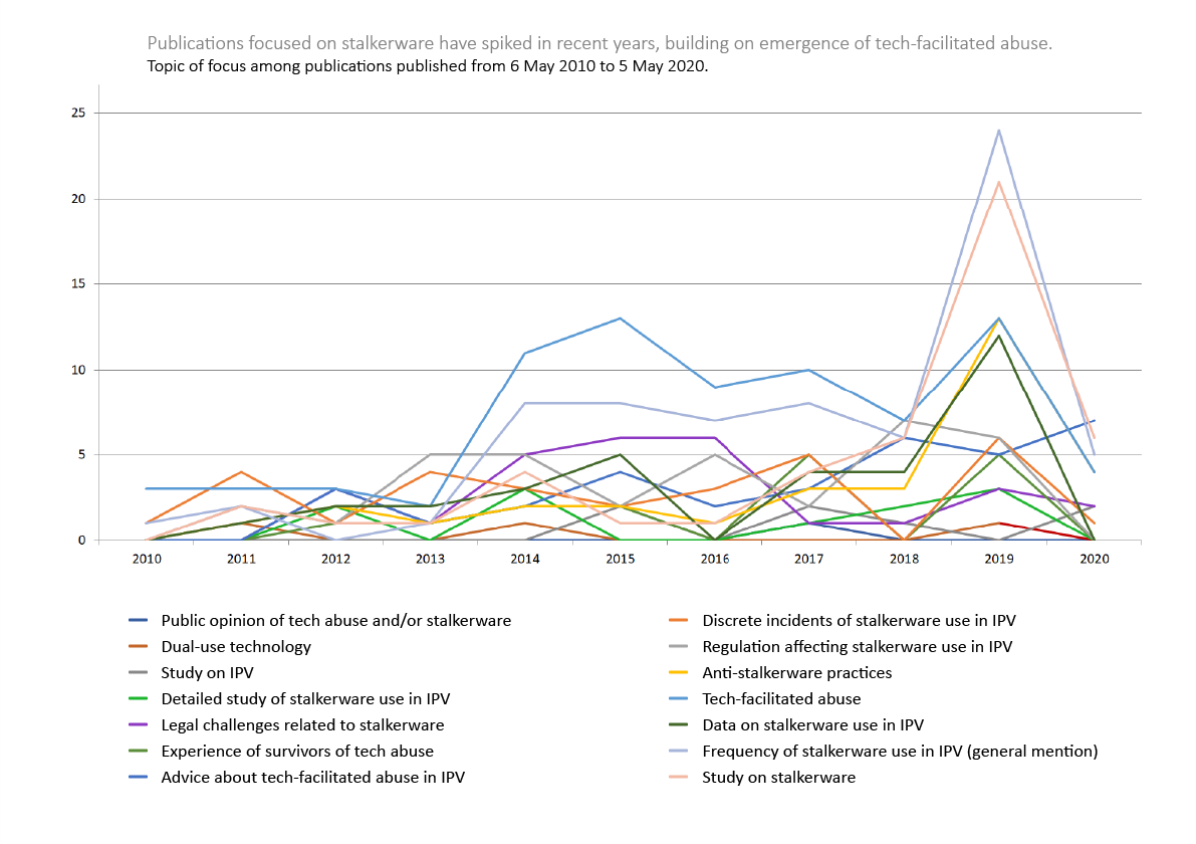


Figure 1. Number of publications by topic of focus from 6 May 2010 to 5 May 2020

Stakeholders and Terms

The terms used to refer to technology for stalking, harassing and related behaviours are shown in Figure 2. These terms referred to the technology itself, and not to its functions. All terms observed in a publication were counted; the highest number of terms used in a single publication was six. A total of 33 terms were used to refer to these technologies across the literature. The most widely used term was spyware, with 184 publications (of all levels of relevance) using the term and an additional set of publications using the word 'spy' (DIY spy software, spy apps). Location-focused terms (GPS, tracking software/ app/device) were mentioned 96 times, social media (social media/networking) 72, and terms using stalk (stalkerware, stalking app) 43 times. These were also the next most prevalent terms. Interestingly, only 14 publications used terms focused on family ('spouseware', parental control/monitoring, child monitoring), though this may have been a limitation of the search terms used in the final query string. Similarly, a number of publications only referenced the technology using the descriptor of 'monitoring', shown below as 'monitoring applications/software' (distinguishing them from 'child monitoring' or 'employee monitoring' since they did not specify a targeted group). Terms using surveillance had much of the same issues, with many just referring to generic 'surveillance tech' or software/app variations. A number of terms that were used only occasionally are represented in the 'Other' category (Figure 2), including: anti-theft app, anti-violence applications, 'creepware', drone, dual-use app, email, employee monitoring apps, instant/text messaging, Internet of Things (IoT) devices, keylogger software, 'nuisanceware', online communication tools, phones, smartphone apps, and smart home security systems.

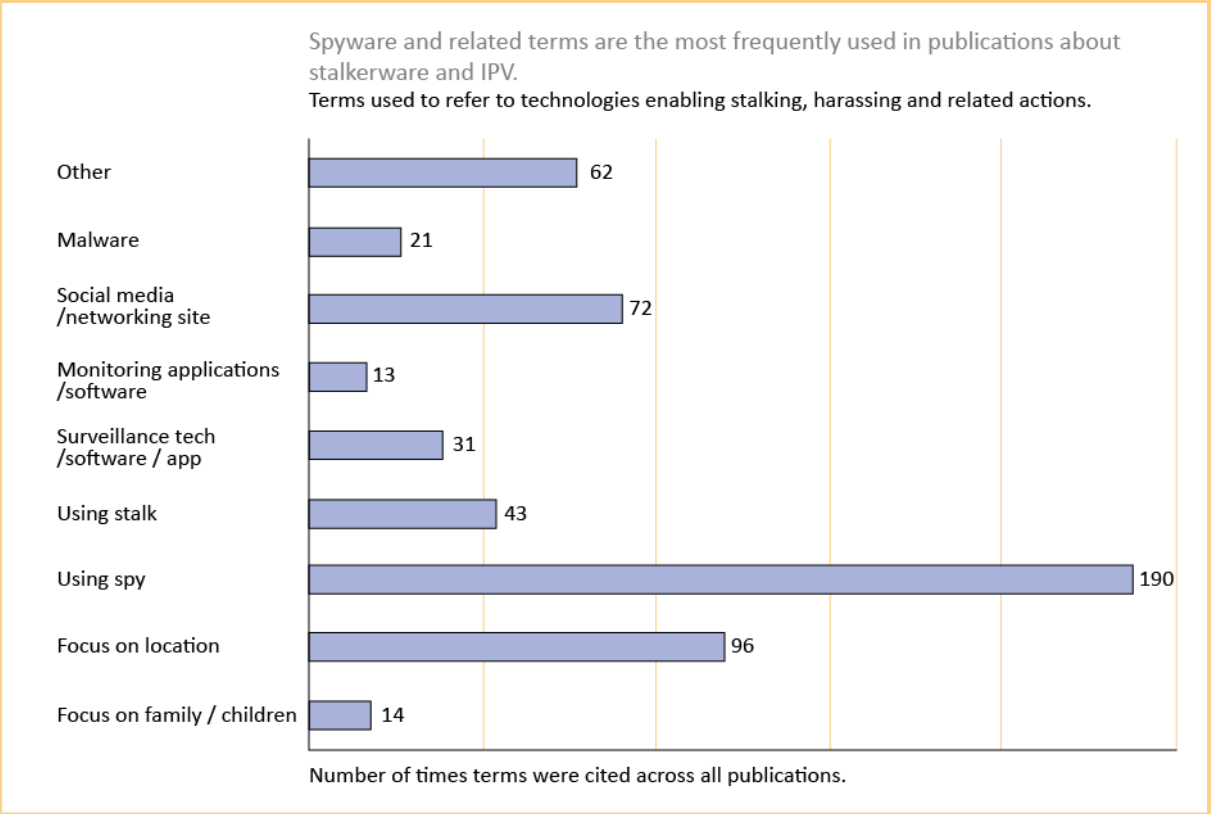


Figure 2. Terms used to reference technology that enables stalking, harassing and related actions

© Tomás Bermudez, Maddalena Esposito, and Jay Neuner

Analysed publications focused on a variety of stakeholders, often engaging with them directly. Of the 228 analysed publications: 21.9 % focused on victims/survivors, 16.9% on perpetrators, 10.9% on policy makers, 8.7% on advocates, 8.7% on the general public, 7.5% researchers, 7.2% on the statutory sector (including law enforcement), 6.5% on support organisation workers, 5.7% on the private sector, 3.5% on stalkerware developers, and 2.5% on anti-stalkerware companies. Importantly, victims/survivors and perpetrators are the stakeholders on which publications focused most often. Anti-stalkerware companies were rarely engaged, though this may have been a limitation of the query string.

Box 1. Notable high-relevance texts

The Many Kinds of Creepware Used for Interpersonal Attacks by Roundy et al. (2020) gives a technical assessment of the capacities of a variety of stalkerware apps. The authors produced a piece of software that carries out detection of stalkerware by applying 'guilt by association' to catch potentially unnoticed software. Their study notes significant similarities in structure and function among stalkerware apps. Their contribution is also significant for its analysis of stalkerware commercialization.

The Spyware Used in Intimate Partner Violence contributes tools for detection and labelling of stalkerware (Chatterjee et al., 2018). Their focus is on the ecosystem of stalkerware apps. Most of the identified apps are classified by the research team as 'dual-use', or apps with an apparently legitimate purpose. The researchers also documented online resources that inform abusers about stalkerware, as well as apps encouraging use of their product for intimate partner stalking through their marketing. Finally, they noted that anti-virus and anti-spyware software consistently failed to detect and address dual-use apps (Chatterjee et al., 2018).

The Consumer Spyware Industry: An Australian-based analysis of the threats of consumer spyware and *The commodification of mobile phone surveillance: An analysis of the consumer spyware industry* – focus on commercial aspects of stalkerware (Molnar & Harkin, 2019; Harkin, Molnar & Vowles, 2020). Their focus is on legislation and regulation with some technical analysis. They delve into the legality of the technology within the Australian context and provide a series of recommendations to public and private actors to address the issue. Notably, the studies were conducted in partnership with the Australian Communications Consumer Action Network (ACCAN), a government-funded advisory body.

The Predator in Your Pocket, by the researchers at The University of Toronto's Citizen Lab, provides the most comprehensive overview of the state of stalkerware technologies and of the research field (Parsons et al., 2019). While the paper is focused on analysing the threat of stalkerware technology and different aspects of it, it also contains a thorough review of key texts like those mentioned above. The text also details research on general tech abuse in intimate partner contexts and highlights that the issue of tech abuse, and in this case stalkerware, has a gendered element, with women being most affected.

The State of Stalkerware in 2019, published by the multi-sector consortium Coalition Against Stalkerware (Kaspersky, 2019) provides a general overview of stalkerware, some statistics on its use, and on location of use – finding Russia, India, Brazil and the US to be where stalkerware is most used. They also noted that there was a 373% increase in detection of stalkerware between 2018 and the same period in 2019.

The advocacy sector also has relevant texts to highlight, notably *Digital Stalking: A guide to technology risks for victims* by Perry in collaboration with Women's Aid and the Network for Surviving Stalking (2012). Its key contributions to the field are its focus on impacted populations, the examples of support and advice offered, and the accessibility of the publication for non-experts. It is also an early publication within our timeframe raising the issue. This highlights the longstanding nature of these concerns. Other texts from advocacy organisations are largely focused on producing guides and tools for survivors, as well as anti-stalkerware practices (Perry, 2012; Laxton, 2014). They are also concerned with the normalisation of technology that motivates stalkers and abusers.

Discussion

The increased interest in stalkerware within general technology-facilitated abuse over the past years, in conjunction with constant growth of journalistic reporting on the issue and the increase in publications on anti-stalkerware practices, points to higher awareness and concern regarding the issue, both amongst researchers and the general public. Little had been written about anti-stalkerware practices or other detection and reporting tools until 2019. This is particularly true outside of advocacy and media publications and even more so regarding direct advice to victims/survivors. This is not only reflected by the topics of focus, but also by the stakeholders of focus, particularly within academic publications. Meanwhile, news media coverage of the issue often uses interviews with stalkerware survivors or with researchers to support their reporting, indicating an intention to both personalise the impact of abstract technology and ground research into stalkerware.

While many academic papers conclude by proposing important policy and legislative changes, and even create useful software for stalkerware detection that could be used by private businesses (Roundy et al., 2020), there are few to no recommendations for individuals or accessible tools for individuals to check whether they are affected by stalkerware. Focus on survivors and perpetrators amongst academic publications is clearly present; however, they are rarely engaged directly, explaining the low use of interviews and other methods that entail personal engagement. The understanding of individual impact and the understanding of the technology are disjointed. This may be part of the broader limitations of IPV research more broadly, with many gaps around the impact on and response to IPV by survivors, and children as reported by the World Health Organisation (WHO, 2018). This limitation makes analysing the use of different technologies in IPV difficult. Equally, there is a lack of cohesion in understanding what constitutes IPV and the extent of its influence (Johnson, 2008).

Researchers in multiple fields are producing knowledge as guidance for potential victims/survivors to guard against or root out stalkerware, like the resources produced by Perry and Women's Aid (2012) or the academic work by Leitão (2019) and Freed et al. (2017). But further cooperation between sectors is needed in this area as anti-stalkerware recommendations remain generally non-technical. Some growth in this realm is expected; for example, an article from *WIRED,* published after our 5 May 2020 search, outlined ways for individuals to check their devices for stalkerware and in some cases offers solutions or ways to get rid of it (Nield, 2020). Yet, while quite comprehensive and approachable, the article does not consider the complexity of the situation in which the affected person affected might be. These connections are also frequently missing from the publications analysed in this literature review, reflecting a broader challenge in integrating insights from across disciplines into critical research on this topic.

There is a critical lack of agreement across the literature on the definition and use of key terms like stalkerware with a variety of new terms like 'creepware' and 'spouseware' created to address the same technology (Roundy et al., 2020; Wells & Klosowski 2020). Moreover, definitions of stalkerware are muddled with the inclusion of different technologies, with some publications even including social media.

There is also complexity to stalkerware in the variety of use, distribution, capacity, marketed intent, and language use of different apps. Several papers, particularly those produced by advocacy groups, also note that stalkerware has a lasting impact beyond the original contact with the technology (Freed et al., 2019; Perry, 2012). This adds another aspect to consider, where more research is needed.

Focusing on the aspect of language use for marketing and talking about stalkerware, several publications indicate concern about the normalisation of stalkerware and general tech-enabled spying practices within intimate partner contexts. Stalkerware producers use vague or misleading language to get around legislation loosely regulating the sector (Parsons et al., 2019; Harkin, Molnar & Vowles, 2020). Notably, this misleading use of language seems to be a trend as it is reported by multiple publications with different geographical focuses. Secondly, policy and legislation practice on the issue of stalkerware seems to be insufficient as of now. Khoo et al. (2019) note that existing laws have the theoretical capacity to be applied, but this has not happened. For instance, in the Canadian context, existing laws governing some aspects of stalkerware, such as data protection, are not being enforced because there is a gap between what is prescribed by law and accessible tools for survivors (Khoo et al., 2019).

While publications note the addressees of their recommendations, there has not been much discussion on which sector or stakeholder should be the target of prioritised action. In Australia, for instance, work in other sectors like image-based abuse research has called for not just legislative action on the issue, but improved education on issues like gender-based discrimination, as well as stronger reporting and support systems for people affected by technology-facilitated abuse (Henry & Powell, 2016). Additionally, the work that has been done directly regulating stalkerware is almost exclusively located in Australia which is likely because of the government investment into addressing technology-facilitated abuse (Molnar & Harkin 2019; Harkin, Molnar & Vowles, 2020).

Finally, some publications also place the analysis of stalkerware and its related technologies within the context of existing conversations around domestic abuse, attempting to look at the impact of technology in these contexts. In their work with Women's Aid, Laxton (2014), notes that the controlling behaviour common in domestic violence or IPV involves a variety of acts that have the goal 'to make a person subordinate and/or dependent.' Several other publications provide similar descriptions of this control and note that it can inflict serious mental and physical harm, enabled by stalkerware and other technologies (Leitão, 2019; Freed et al., 2019). Just as similarities in definitions seem useful in gaining a shared of understanding of stalkerware, a shared definition in the broader context of domestic violence has also been raised as an important need for future policy development and targeted actions – as emphasised by a representative of Women's Aid UK in oral evidence about a draft domestic abuse bill in that region (UK House of Commons, 2019). Some publications also discuss how stalkerware use in IPV, as part of the broader context of IPV, is considered by them a gendered problem affecting women more so than other groups (Parsons et al., 2019).

Ultimately, as of now there is low understanding of the extent to which stalkerware is used in IPV. Some aspects of it that are under-unexplored include: the number of apps produced, the number of companies producing stalkerware, the number of users, the number of people affected, and the duration of the impact of stalkerware use in IPV.

STUDY 2. INTERVIEWS

Study 2 is a set of interviews with researchers and practitioners working on and around stalkerware and IPV. The aim of Study 2 is to gain expert opinions on the state of knowledge on stalkerware and IPV.

In particular, the objectives of the study are to (1) gauge areas of consent and disagreement on the terminology relating to stalkerware; (2) to understand current research and policy across different sectors, namely, academia, the media, the voluntary sector, the statutory sector, and the tech sector; and (3) to identify any research and policy gaps for the research community to address. Finally, the insights of Study 2 were used to inform the survey items of Study 3.

Methods

Study 2 was designed as a set of semi-structured interviews to generate qualitative data pertaining the state of knowledge on stalkerware and IPV. Each interview included 28 questions. The questions were initially designed on the survey questions Jarvis and Macdonald's paper. The interview questions were then modelled after insights drawn from the literature review, after conversations with our client Chayn and the advice of our supervisor, Dr Tanczer. The design of the interview was intentionally semi-structured in order to allow flexibility for both the interviewees and the interviewer to expand on specific answers.

The final questions related to: the participants' backgrounds; the definitions and terminology related to stalkerware; the participants' opinion on current and future research; the participants' concerns related to stalkerware and their perception of the main hurdles to mitigate its malicious use; the participants' knowledge of resources and organisations on stalkerware and IPV; and the participants' perception of other sectors' work. The interview questions can be found in Appendix D.

Sampling Method

Interview participants included researchers, practitioners, and experts working in cyber security, IPV, and technology-facilitated abuse across academia (including PhD and postdoctoral researchers), the voluntary sector, the statutory sector, the tech sector, and the media. We set an exclusion criterium of age ranging from 18 and 70.

Participants were identified in four phases through four sampling methods. Initial contacts were identified by Dr Tanczer, by Chayn, and by two other professional acquaintances of Dr Tanczer's. Further contacts were identified through key publications in our literature review. The last batch of potential participants was snowballed from the first interviewees at the outset of the interview round. Lastly, some participants approached the research team after the team members advertised the research on their personal Twitter profiles. At the end of this identification process, the number of potential participants was 103.

After doing so, we excluded any contacts whose primary focus was not stalkerware use in IPV, and all those candidates whose contact details were not available. We then invited 49 contacts to participate via email. We received a response rate of 46% and completed 23 interviews.

Of the 23 participants, 39% (nine) were based in the US, while 21.5% in the UK, 17% in Australia and 8% in Canada. Less than 5% of interviewees were based in other regions, such as France (one), Greece (one) and the Russian Federation (one). The majority of the interviewees (56%, 13 respondents) had an academic background. 21% worked in the tech sector, while the media and the voluntary sector had a representation of 8% each. Only one participant worked in the statutory sector.

In terms of focus of work, 39% of the interviewees focused mostly on tech abuse in general (nine respondents) and 34% on the functions of stalkerware. Another prominent area of focus was the experiences of survivors of tech abuse (15%). The legal and policy implications of stalkerware and the experiences of perpetrators of technology-facilitated abuse had minor representation (4% each).

Data Collection

The interviews were conducted from 22 June to 22 July 2020, running for one month. We had initially planned to run the interviews for two to three weeks, and to conduct a second round of interviews after the survey. However, to better allocate time to the survey and to the analysis of the three studies, we decided to run one, longer round of interviews.

The interviews were conducted by all the research members. Some interviews were conducted by two research members, while the majority were conducted individually. Interviews took place online, mainly over Microsoft Teams, Google Meet, Signal and Skype. Before taking part in the interviews, participants were given a participant information sheet, containing information about our research and about the interviews, and a consent form.

All interviews except one were audio-recorded with permission of participants. The recorded interviews were transcribed prior to analysis through Microsoft Teams' automatic transcription service, or manually when using Google Meet, Skype and Signal; the non-recorded interview was transcribed manually.

Analysis Method

The analysis of the interviews was underpinned by a thematic analysis method. Thematic analysis is a qualitative research method to identify, organise, analyse and report themes from large bodies of qualitative data, such as interviews (Braun & Clarke, 2008). This method is apt for group-based research and allows flexibility to researchers to categorise and interpret the data without losing its richness (Braun & Clarke, 2008). Moreover, this method was deployed to analyse interviews in previous qualitative work on technology and IPV (Freed et al., 2019; Woodlock, 2017; Tseng et al., 2019).

Taking a cue from Nowell et al. (2017), our thematic analysis was conducted in sequential phases: extensive familiarisation with the data, generation of initial codes, the identification of themes and sub-themes within the coded dataset and the final reporting.

Prior to familiarising ourselves with the data, we generated codes to summarise relevant information we were seeking into a shared matrix. The coding was developed deductively from the main interview questions around which our enquiry was designed (Table 2). Codes referred to the interviewee's background; opinion of current and future research on stalkerware; definitions and understanding of stalkerware; concerns and opinions of hurdles to mitigate stalkerware; and opinion of other sectors' work.

Excerpt	Coded for	Theme	Sub-theme
'[It] is just the overwhelming and daunting cultural change it would take for people to ever consider activity like this illegal because we've essentially normalised surveillance in so many different aspects.' [p. 21] *Megan L. Brown, University of Arizona*	Top concerns about stalkerware	Concerns and hurdles to mitigate stalkerware	Normalisation of surveillance

Table 2. Example of theme and sub-theme development in interview coding

After reaching a clear set of codes, we familiarised ourselves extensively with the interview transcripts. At this stage, each of the researchers inductively generated key overarching themes across the coded dataset and recurring sub-themes in each of them. We then triangulated our individual results and reviewed and refined them until reaching consensus. After this stage, the overarching themes were narrowed down to three, namely 'Definitions and Terminology', 'Research' and 'Concerns and Hurdles to Mitigate Stalkerware'. Both the coding and the development of the concepts and themes were revised iteratively, as we engaged with the interview transcripts iteratively.

Results

Definitions and Terminology

When asked to share a definition of the word 'stalkerware' the interviewees gave different responses, but with some common recurring characteristics pointing to the intention of technology design and use, to consent, to victims' awareness and to access to a device.

The most used terms amongst the interviewees was 'stalkerware', while the second most used word was 'spyware'. Other terms used by the interviewees were: 'spouseware' (two interviewees), consumer spyware (one), family monitoring software (one), parental control apps (one), 'creepware' (one) and *logiciel espion* (one) in the French language.

Stalkerware was referred to most commonly with the terms 'technology', 'app' and 'software', although there was a lack of consensus as to what technologies actually fall within this definition. Mostly, stalkerware was referred to as an 'app', such as mSpy, FlexiSpy, RetinaX, which could be installed on a mobile phone, desktop or tablet. Such apps include software that is branded as parental monitoring software, which may be repurposed and misused to perpetrate abuse on a partner. Some interviewees, however, recognised the ambiguity of the term 'stalkerware' and included in this category a broader set of technologies, such as GPS trackers, IoT devices, social media and applications like Find My Friends and Google Maps, all of which may be misused to perpetrate intimate partner abuse. Adam Molnar from the University of Waterloo, for instance, reflected: 'The primary function [of] IoT devices isn't about targeting or monitoring specific individuals for tracking, but they can be used that way. Whereas parent, child, monitoring or stalker applications do have that primary function.'

Relatedly, one noted characteristic of stalkerware was the surreptitious and covert mode of surveillance and the lack of consent and awareness on the victims' side. Other interviewees, instead, maintained that stalkerware is a legitimate product, that can be used maliciously to

perpetrate abuse, and that, therefore, is not solely based on the victims' lack of consent or awareness, as in the case of parent monitoring software.

Nonetheless, interviewees stated that stalkerware infections occur more rarely than it is thought, and often victims' feeling of being monitored boils down to account compromise, which occurs due to poor privacy and security practices. Eva Galperin of the Electronic Frontier Foundation (EFF) said: 'Often [a victim's] problem is not stalkerware, it's almost always account compromise or a leak of information that they're not aware of, a friend who was leaking information. This happens all the time. So, it is very rarely stalkerware. But when it is, it is especially scary.'

Another noted characteristic of stalkerware was the need to physically access a victim's device in order to install it and gather information surreptitiously. When confronted with the linguistic ambiguity between spyware and stalkerware, interviewees noted that stalkerware implies the specific setting of IPV, and a specific set of threats as opposed to spyware, which was referred to as a more generic, umbrella term to refer to government-style surveillance software or to private use surveillance software to obtain a victim's financial information. Moreover, spyware can be installed remotely while, again, stalkerware must be installed by means of physical access to a device.

Research

From the analysis of research-oriented answers, we identified three main themes pointing to the value of multidisciplinary approaches in current and future research, to research gaps, and to victim/survivor-centred research.

The majority of respondents felt that current research is doing particularly well in raising awareness and putting the issue on the policy agenda, while some felt that this is a shortcoming of the current research field, especially within law and technology-related disciplines.

Interviewees also felt that the collaborative and multidisciplinary nature of the field was a positive aspect of the current research field, especially the collaboration with the voluntary sector and with victims/survivors. In this regard, interviewees mentioned specifically the research produced by Cornell University and New York University, by University of Toronto's Citizen Lab, by Deakin University with support from ACCAN, and within the Coalition Against Stalkerware. One interviewee felt that there is, however, room for better collaboration between computer science, information security and the social sciences disciplines, especially criminology, within academia. Another interviewee noted that there is room for international cooperation and policy learning, specifically from Australia's eSafety Commissioner.

Research gaps within the current research field related to under-investigated topics, such as detection capabilities, legal and policy analysis, the developers' ecosystem, financial abuse, and the privacy and security decisions that inform the design of devices. Relatedly, according to the interviewees, future research should focus mainly on investigating the market and the prevalence of stalkerware, as well as on legal and regulatory interventions to limit its market. Some other interviewees believed that future research should focus on improving anti-virus detection capabilities, on telecommunications systems, and on mobile phones' operating systems.

Importantly, researchers commonly pointed out the need to focus research efforts on both the impact on victims/survivors and on perpetrators' experiences, as these are under-researched topics within the realm of stalkerware and IPV. Interviewees also felt that

victim-/survivor-centred research would provide a sound evidence base on which efforts to counter stalkerware should be based.

In line with the future topics of research, interviewees were most interested in seeing qualitative methods used, in particular interviews and workshops, field research and participatory research with victims/survivors of abuse and perpetrators. However, one interviewee believed that interviews might not always be a helpful method of enquiry, in that victims/survivors might not be aware that their device has been infected with stalkerware. Technical analysis on victims' devices and reverse engineering to identify stalkerware was encouraged, although reservations were expressed in this regard due to the potential lack of immediate value to victims/survivors.

Concerns and Hurdles to Mitigate Stalkerware

The interviewees expressed shared concerns in relation to stalkerware and IPV. The main themes that emerged were: the lack of awareness across all sectors and in the general population; the normalisation of surveillance; the legitimacy and legality of the technology; the impact of stalkerware on individuals in a situation of abuse; the lack of expertise and resources in the support organisations and law enforcement; availability and design of technologies; and notification.

General awareness of the topic was deemed as a concern and a hurdle to mitigate the malicious use of stalkerware and IPV. Interviewees thought that the lack of awareness in their own fields and in the general population should be improved in order to counter stalkerware effectively and in order to provide effective aid to victims/survivors. For instance, Thomas Ristenpart of Cornell Tech reflected: 'The best advice for what to do about stalkerware before the last few years was, "Throw away your phone if you thought it was acting funny", which of course is not a very good solution for a number of reasons.' Some interviewees were additionally concerned about the role of some media in promoting false narratives and sensationalising stalkerware as a technology that requires much more sophistication than it does, agitating fears in individuals at risk.

The normalisation of surveillance in intimate relationships and in everyday life was also noted as particularly concerning by interviewees, and it was linked by some to the difficulties in urging policy and legislation to address stalkerware in IPV.

As Megan L. Brown from the University of Arizona stated:

> '[It] is just the overwhelming and daunting cultural change it would take for people to ever consider activity like this illegal because we've essentially normalised surveillance in so many different aspects.'

Interviewees also mentioned that the legitimacy of some technologies – especially of those whose primary use is not monitoring or tracking – represented a hurdle in countering the malicious use of stalkerware in IPV. Relatedly, the legality in which these products are built, marketed and sold (independent of the geographical context) was seen as a major hurdle to counter the use of stalkerware in IPV. However, the fact that many of the functions of, or activities enabled by, stalkerware apps may already be illegal was also cited as a mechanism for law enforcement.

Eva Galperin (EFF) noted:

> 'Frequently, the people who are using these products are already breaking the law. They are already breaking lots of laws. All we need to do is to enforce the laws that already exist.'

Interviewees also shared their concerns about the 'real-life' impact that stalkerware might have on individuals in situations of abuse. Stalkerware abuse might in fact escalate in physical violence and homicide, in financial abuse, and might endanger individuals close to the victim. Moreover, interviewees flagged bad data storage practices among stalkerware companies as another risk, as exfiltrated personal data affecting a victim/survivor may be accessed by malicious third parties even outside of a situation of abuse.

A core issue to work in this field is the lack of resources and technical expertise in the voluntary and statutory sectors. Interviewees felt that support organisations often lack the appropriate technology training to deal with technology-facilitated abuse, despite being the best suited to help individuals in need. Interviewees pointed out that this is a constraint that often comes from the voluntary sector's lack of resources and funding. Similarly, participants stated that police forces are often ill-equipped to address stalkerware abuse and that law enforcement is often unresponsive and not collaborative on cases of IPV and domestic violence – a concern that was shared in relation to the judiciary as well.

Joseph Cox of media outlet VICE said:

> 'When it comes to law enforcement or police, there are just very, very few convictions for the use of this software, which in a lot of cases, if not the majority, is going to be quite clearly a crime. Whether that's going to be wiretapping laws, or hacking laws, or whatever it may be. There are just so few convictions around this, [which] is where I would say law enforcement is kind of falling short.'

Some interviewees also noted the wide availability of stalkerware on Google and Apple app stores and the ease of deployment of the technology, and that the design of some mobile phones' operating systems is more susceptible to stalkerware than others. Yet the often-covert nature of stalkerware was also indicated as a challenge for victims to understand any risks they are facing, particularly with anti-virus detection capabilities being under-developed and uncommon. The fast evolution of these technologies was also cited as a risk, posing challenges to any newly identified detection or countering effort. But even these detection mechanisms themselves may be risky; some interviewees mentioned that installing anti-virus detection solutions to scan a device might be picked up by stalkerware apps, potentially putting the victim in greater danger.

One interviewee shared that a main hurdle is notification and the usability of devices, specifically, how to notify users that a legitimate piece of software is being misused against them.

Rahul Chatterjee from the University of Wisconsin-Madison stressed:

> 'Notification is [a] big concern. How do you notify the people that [they] were being stalked or spied on without annoying them? If you send too many notifications, there will be notification fatigue and people will stop reacting to that.'

Relatedly, the usability and privacy and security design of technologies were seen as a hurdle to mitigate the malicious use of technology to perpetrate abuse. For instance, one researcher from University of the Arts London believed that rigid privacy and security settings, especially of shared devices, might hinder victims' attempts to escape a situation of abuse.

Discussion

A set of key conclusions can be drawn from our analysis, which resonates with previous and current work on technology-facilitated abuse and IPV.

Firstly, there is a need to have an agreed, universal definition of stalkerware, without which it will be difficult to concentrate research and policy efforts. Recent work from the Coalition Against Stalkerware set out a definition of stalkerware as 'software, made available directly to individuals, that enables a remote user to monitor the activities on another user's device without that user's consent and without explicit, persistent notification to that user in a manner that may facilitate intimate partner surveillance, harassment, abuse, stalking, and/or violence' (Coalition Against Stalkerware, 2020). This is an important step, which should be recognised by policy and law in any regulatory or legislative endeavours.

This definition should also be recognised by law enforcement agencies and the judiciary when dealing with stalkerware use in IPV. As highlighted in our analysis, in fact, law enforcement and the judiciary lack technological awareness to be able to understand and address stalkerware abuse. Lack of awareness, along with poor training and resource allocation to the statutory sector is the reason why the work of this sector has been unhelpful towards stalkerware abuse victims. Previous multidisciplinary qualitative work on technology use in IPV has found similar results. Freed et al (2017) in their *Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders* claim that there is little technology expertise in legal systems – one ramification of it is that there are very few recourses for those experiencing technology-facilitated abuse.

This latter point relates to our interviewees' concerns regarding the cultural shift needed in the statutory sector in order to entrench technology-facilitated gender-based abuse in policy and legislation. In this sense, awareness raising efforts should not be circumscribed to a particular geographical context or sector but should be a continuous and iterative effort especially as the sophistication of technology and of detecting capabilities will change quickly. In *The Predator in Your Pocket,* Parsons et al. (2019), who employed a multidisciplinary and multi-stakeholder analysis to the stalkerware ecosystem in Canada, have found comparable results: awareness raising would be most effective amongst frontline workers providing support and the general population. Parsons et al. (2019) also believe that the development of legal and policy responses to stalkerware abuse should be based on better legal education in the general population.

Relatedly, a key insight of our interviews is that there is a gap for cross-sector collaboration and knowledge transfers, especially between academia and the voluntary and statutory sectors, and within these, especially in support organisations and police services. Previous work on technology-facilitated intimate partner abuse by Leitão (2019) also points to this. Her work stressed that knowledge transfers and training between police services, support organisations and victims themselves would be beneficial, especially with regard to capture and storage of digital evidence. As our interviews showed, academia, and research more broadly, would be best placed to provide an evidence base into victims/survivors' and perpetrators' experiences and into the needs of the support sector to respond effectively to stalkerware. Freed et al. (2019) similarly emphasised the role of academics and technologists in assisting frontline workers within support services, as well as case workers and lawyers.

Cross-sector collaboration would be beneficial for the development of responsible technologies. As emerged in the interviews, technological responses, such as anti-virus detection tools and technology design decisions should also be mindful of how the tech can be misused and should focus on protecting users from escalation of abuse. Leitão (2019) and Freed et al. (2017; 2019), similarly pointed to how privacy and security settings and user interfaces could be co-designed by a broader range of stakeholders, including support sector workers. In this sense, the reactive approach of law enforcement and of support organisations should be paired with a more preventative approach on the tech sectors' side.

Our interviewees finally reflected on how IPV is a complex, socio cultural issue of which stalkerware and technology are only a part. Any policy and legal responses and any interventions addressed to victims of technology-facilitated IPV should not engage in victim-blaming or be unhelpful to those in danger, such as advice that frames the cessation of abuse as a victim's responsibility to stop using technology. It is also important that any advice does not provide abusers with further means to perpetrate violence. Freed et al. (2017; 2019) and Parsons et al. (2019) have also found that such advice might endanger victims further, other than isolate them from support systems and economic opportunities. Importantly, Parsons et al. (2019) state that policy and legal responses should not ask victims to compromise between their 'physical and psychological safety, personal freedom, and autonomy'. In other words, any technological responses and interventions should be commensurate to the victims/survivors' needs and wellbeing.

STUDY 3. SURVEY

Study 3 complements the earlier studies by qualifying the previously identified knowledge on stalkerware use in IPV contexts among self-identified researchers and experts. Statements, sentiments, and themes in the field were collated from the literature and interviews, then presented in an online survey for response and reflection from respondents.

Methods

The target participant pool for the survey was researchers working on and around cyber security, IPV/domestic abuse, and technology-facilitated abuse who had direct knowledge

about the use of stalkerware in IPV contexts. The survey was openly accessible online, so we requested participants self-identify.

The survey consisted of 33 questions, developed through an iterative process. Foundational questions about the field were first identified from the literature. These were refined through insights from the interviews, and additional questions were subsequently scoped from the interviews. The questions aimed to identify: (1) background information about the participants; (2) context about their knowledge of stalkerware use in IPV, framed within contexts identified from the literature review and interviews; and (3) their perspectives on the field of research into and activity around the issue of stalkerware use in IPV. Where possible, open comment boxes were made available for participants to provide additional context on their responses. The full list of survey questions can be found in Appendix E.

The survey was hosted and distributed online via the platform Opinio. This approach was selected to ensure efficient data collection and analysis, to ensure safety during the co-occurring pandemic, and to potentially scale our reach beyond our known contacts.

To reach a broad pool of potential participants, we distributed and promoted the survey across multiple channels, notably on Twitter and on email newsletters to which our team's network was connected (including through our project supervisor, client contact, and university department). We also reached out directly to past interviewees and potentially relevant researchers identified from our literature review, requesting their participation and their assistance in distributing the survey more widely. We also encouraged participation from attendees at an external conference in which we participated in late July 2020. The survey ran from 27 July 2020 to 10 August 2020, a total of 16 days.

The respondents self-identified across 12 countries and territories, with the 63.64% or 35 respondents noting they worked in the US. A further concentration of 10.91% and 5.45% identified themselves as working respectively in the UK and Australia. The largest proportion noted that their work covered the US (23.38%).

Participants were primarily from academia (28.57% or 14 respondents), the statutory sector (8.16%), the voluntary sector (38.78%), and the tech sector (12.24%). Notable concentrations of academics identified their disciplines as social work (25%) and engineering/computer science/cybersecurity (18.75%).

Results

We received 49 total responses to the survey. The following highlights some key results.

Defining Stalkerware

The survey first aimed to coalesce shared definitions in the field through frequency of terminology used, rating of importance, and level of agreement with provided statements about stalkerware and its use in IPV.

When asked to share their own definition of stalkerware, some commonalities emerged. 'Software', 'apps', and 'technology' were the most used words referring to stalkerware, with some use of the term 'malware'. These sometimes appeared in conjunction with the terms 'malicious' and 'legal'. 'Tracking', 'monitoring', 'locating', and 'collecting data/exfiltrating data' were the primary associated actions.

A smaller subset of the definitions included some of the following elements:

- whether the app, software, or technology was designed specifically for the purpose of actions associated with IPV, with some contrast made to technologies with these functionalities but not their intent (e.g. 'dual-use apps');
- whether the victim was aware of its installation; and
- whether the victim consented to its installation.

Respondents across all sectors overwhelmingly indicated that stalkerware and spyware were the terms most frequently used, from amongst a provided list (Figure 3).

Figure 3. Frequency of terms used in reference to stalkerware use in IPV

More than 50% of respondents selected the following elements as 'most important' to the definition of stalkerware (listed in order of most to least frequently selected):

- 'accessing the device user's personal information', tied with 'monitoring on-device activity';
- 'location tracking';
- 'accessing files on a device';
- 'targeting someone known personally by the app user';
- 'controlling on-device activity';
- and 'key logging'.

In open comments, some respondents also flagged that access to device features and applications, not just files, was an important element to them.

In categorizing stalkerware, respondents broadly agreed (indicated by 'Agree' or 'Strongly Agree') that stalkerware is software installed on a mobile phone (89.8% cumulatively) and software installed on a laptop/tablet/PC (83.68%), and that this category includes GPS

tracking devices (77.55%). There was still a relatively high proportion of consensus that stalkerware included social media and smart home devices/Internet of Things devices, but mixed opinions about drones (Figure 4).

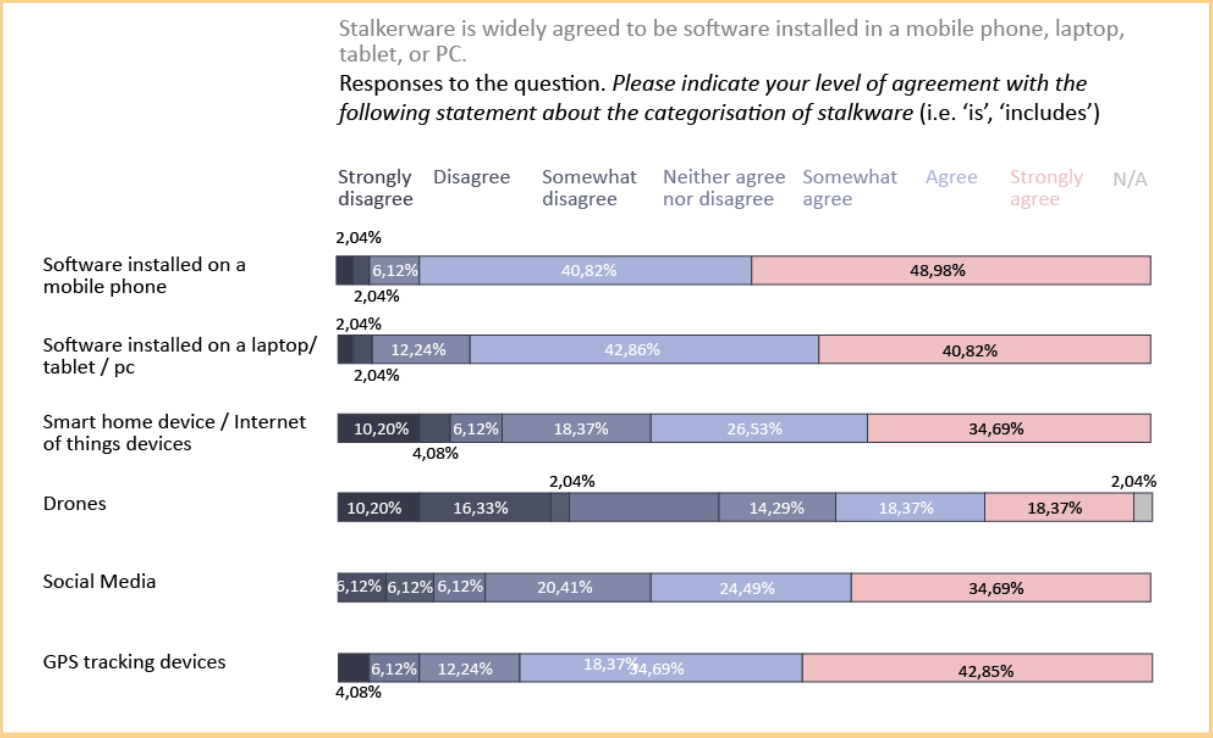


Figure 4. Categorisations of stalkerware

A relatively high proportion (22.45% each for 'Disagree' and 'Strongly disagree') disagreed that stalkerware only operates covertly; an even higher proportion agreed that it operates both covertly and overtly (28.57% each for 'Agree' and 'Strongly disagree') (Figure 5).

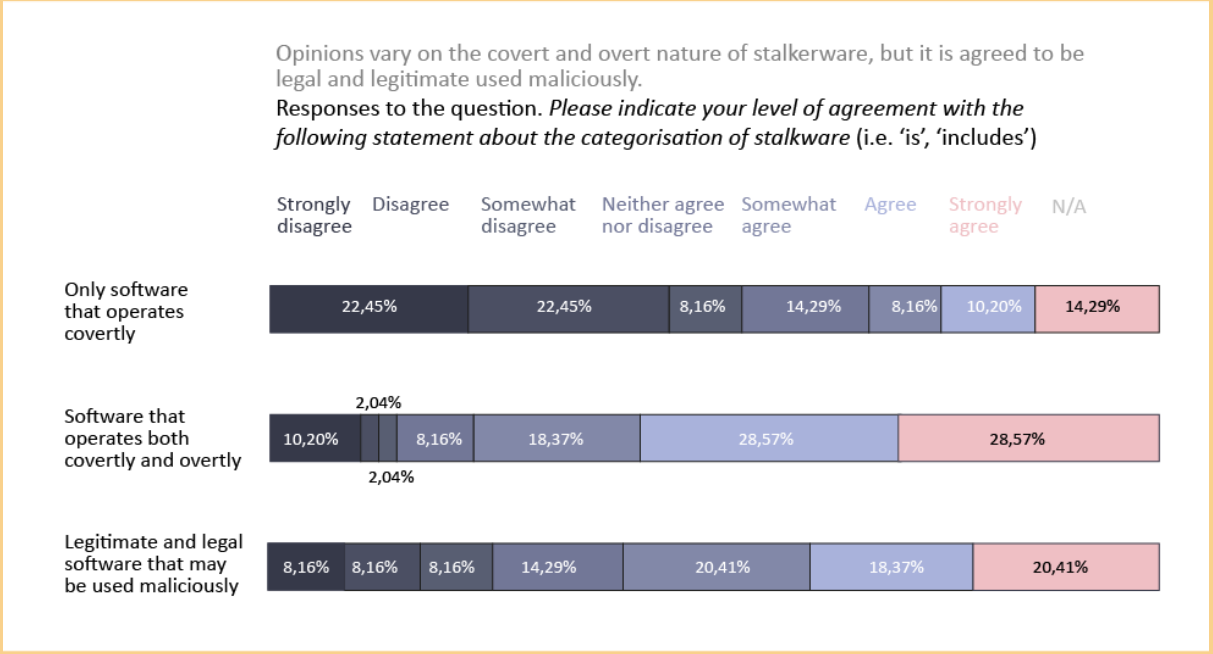


Figure 5. Categorisations of stalkerware (continued)

In contrast, on characteristics of stalkerware, there were the highest levels of consensus (indicated by 'Agree' or 'Strongly agree') about whether stalkerware is software that aims to gather information surreptitiously (46.94% and 34.69%, respectively), and that it is primarily concerned with monitoring on-device activity (38.78% and 30.61%) (Figure 6).

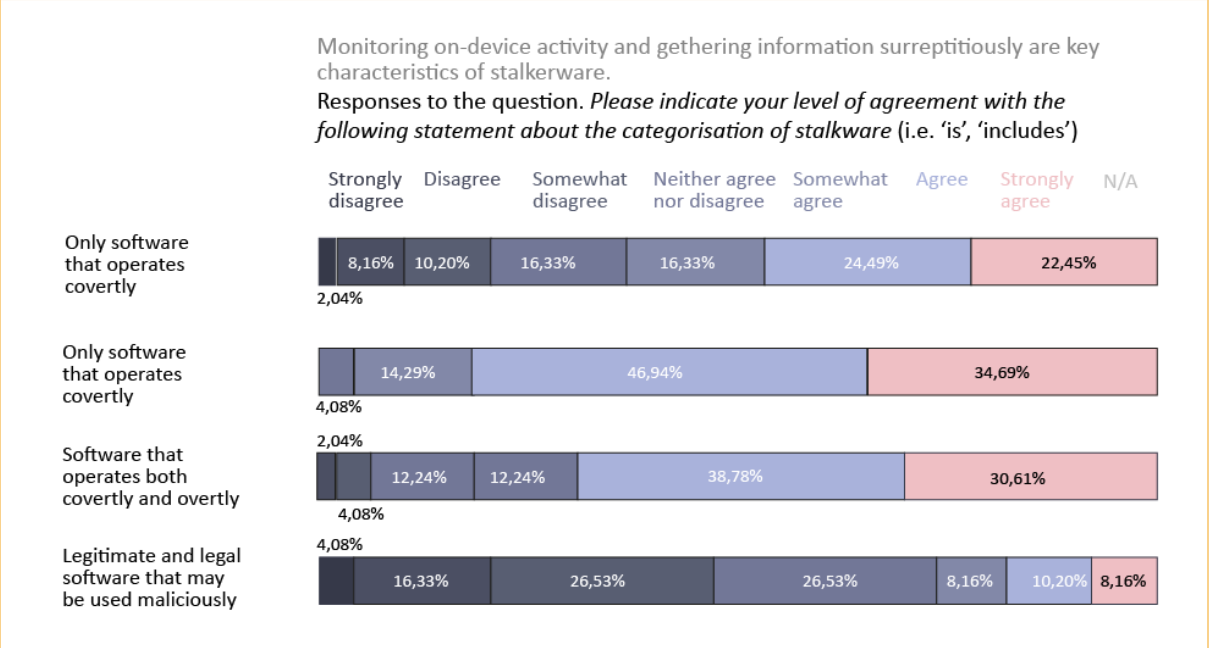


Figure 6. Characteristics of stalkerware

The majority of respondents also indicated some level of agreement with the statement, 'There are some legitimate uses of the functions primarily associated with stalkerware, notably: monitoring on-device activity, controlling on-device activity, restricting on-device activity, or tracking device location' (63.27%). Some respondents mentioned in the open comments that legitimacy was, to them, only for specific features or uses – particularly, parental controls. Some also noted legitimacy, to them, hinged on consent.

We also asked respondents to reflect on the importance of a specific and widely agreed definition for a given sector. Only the statutory sector received a majority of opinions that this was 'Extremely important' (46.94%), followed by the tech sector (40.82%); other sectors were generally distributed evenly between 'Moderately', 'Very', and 'Extremely' important. One respondent commented that they indicated this for the statutory sector for the reason of 'holding people accountable for breaking a law'.

Current Knowledge on Stalkerware

In reflecting on their own knowledge and the current state of knowledge on stalkerware, there was no overwhelming trend for when respondents first learned of the issue; the highest number of responses were 2016 (14.29%), 2018 (10.2%), and 2017 (8.16%).

The majority of respondents said they believed the US was leading the research field on stalkerware (26.21%), followed by the UK (11.65%).

For all identified limitations to current research on stalkerware, more than 60% of respondents indicated the following were 'Moderately', 'Very' or 'Extremely important':

- 'access to data' (cumulatively 77.55%);
- 'lack of industry collaboration with researchers' (71.43%);
- 'lack of government collaboration with researchers' (67.35%); and
- 'lack of financial support/resources' (67.35%).

There was little consensus on various statements probing gendered effects of stalkerware use in IPV, except that the majority 'Agree' or 'Strongly agree' that stalkerware has the greatest impact on people who are female (67.35% cumulatively).

Future Research on Stalkerware

Far and away, the future research topics deemed most important by respondents (with more than 80% of respondents stating they were 'Very' or 'Extremely important') were:

- 'data on the prevalence of stalkerware use in intimate partner violence', 'insights from survivors/victims on their experience', and 'understanding of how to improve frontline support' (each 93.88%); and
- 'mapping and analysis of legislation targeting or related to the use of stalkerware' (81.64%).

Almost all respondents deemed victims/survivors as a 'Very' or 'Extremely important' stakeholder group focus of future research (95.92% cumulatively).

Assessing the Risk of Stalkerware

The vast majority of respondents (approx. 80% or higher) were extremely concerned about the following risks of stalkerware: 'normalisation of surveillance of intimate partners' (83.67%), 'risks to personal physical safety' (87.76%), 'risks to personal mental safety' (85.71%), and 'risks to safety of dependents' (79.59%) (Figure 7).

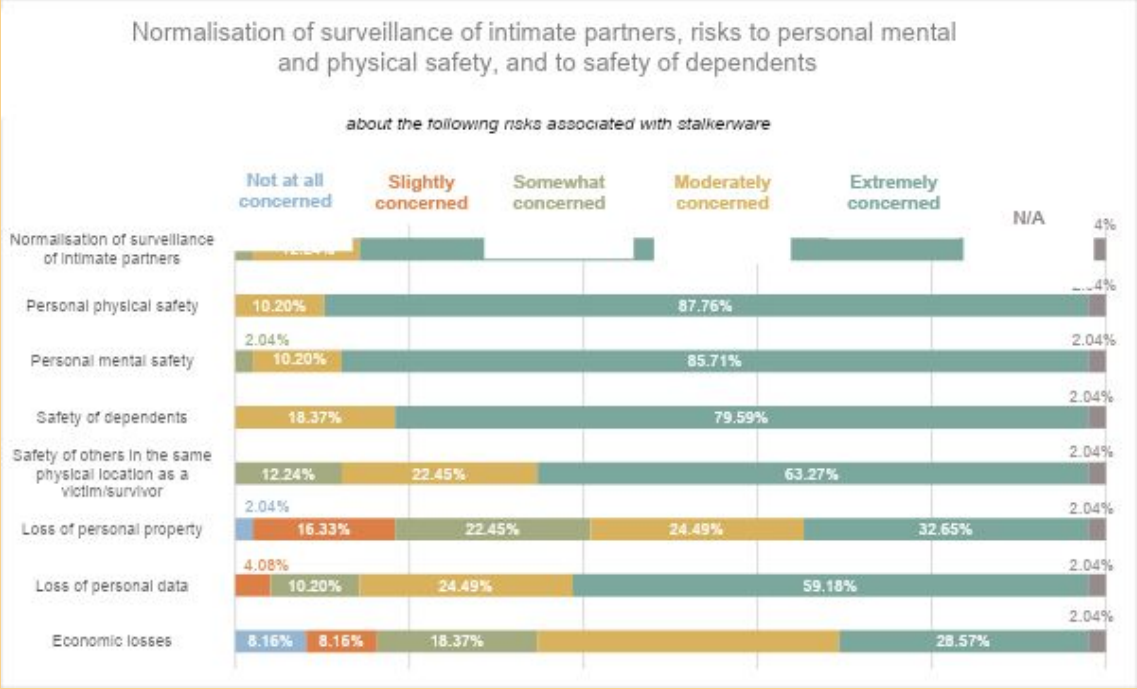


Figure 7. Concerns about risks associated with stalkerware

Countering Stalkerware

Approximately 70% or more of respondents rated 'providing victims/survivors with knowledge on how to detect and act upon stalkerware' (75.51%) and 'providing frontline workers with knowledge on how to detect and act upon stalkerware' (69.39%) as 'Extremely effective' potential measures to counter the use of stalkerware. In reflecting on the other measures, some respondents commented that the statutory sector may be hindered by what was perceived as a lack of prioritisation or helpfulness in dealing with victims of IPV.

A majority of respondents (80% or more) felt that the following sector-specific actions were 'Extremely important': within the statutory sector, 'seeking out and prosecuting perpetrators of stalkerware-based IPV' (85.71%); within the voluntary sector, 'recruiting frontline workers with cross-cutting knowledge' (83.67%); and within the tech sector, 'increasing development of technological safeguards to prevent stalkerware use' (83.67%).

Discussion

The survey revealed a few key trends related to both the state of knowledge on stalkerware use in IPV and consensus around this knowledge.

While the respondents held a broad base of experience, there was no clear turning point in time to indicate a shared surge in awareness. There is consistency in the representation of research expertise from the US and the UK, as well as dominance in the field from those regions. However, this may also speak to the English-language bias of our research and the snowballing of contacts from some individuals and institutions with which we engaged in earlier stages of this research (see 'Limitations and Challenges').

Across the research field as surveyed here, there is disagreement on shared definitions and categorisations of stalkerware, although the high level of frequency attributed to 'spyware' and 'stalkerware' is particularly notable. Another notable area of consensus was the exclusion of certain types of technologies, specifically drones, from the definition of 'stalkerware'. However, in the context of rapidly developing technologies, disagreement about the inclusion of one technology over another within this category may be a limited insight. Recent scholarship has noted how any number of technologies can be part of the actions of domestic abuse and stalking. Woodlock (2017) reflects the insights of other scholars that technologies offer 'more tools and greater scope' for actions targeting victims. In this regard, an awareness that any technology might be used for the activities broadly associated with stalking might have led respondents to be more or less inclusive of technologies under a broad definition of 'stalkerware'.

An interesting area of disagreement around definition is the inherent covertness of stalkerware. Opinions about this varied, including the interpretation of the software acting surreptitiously. Both user's awareness of the technology and whether they consented to its use may be important to develop further. Notably, the relative covertness of a technology and its features and functions is a broader concern around harms stemming from technology use; even though many technologies are required to provide detailed terms and conditions for one's consent, these are difficult for the average person to read and understand, and certain actions might still be occurring in a seemingly covert way, though one might object to it if the action were more overt (Berreby, 2017). It must be borne in mind that these technologies are fully integrated into every part of our lives, from phones with tracking capabilities and cameras, to homes with 'smart' functions. Because of their pervasive presence in everyday life, they become somewhat covert and provide many

avenues of vulnerability to exploitation, harm, and abuse (Freed et al., 2017; Lopez-Neira et al., 2019; Heartfield et al., 2018). They are also part of a growing consistency of surveillance technologies that are part of everyday life (Winder, 2020).

Among the survey responses, the question of consent was in some cases tied to questions of relative 'legitimacy' of a particular function of stalkerware or even the technology or application itself. The relevant question in the survey asked about legality and legitimacy in combination with its malicious use, and there is likely some nuance to interpretations about what is legal and legitimate and how to frame malicious use (for example, intent). Consent alone already plays a role in legal definitions around technology use and abuse, as established by the European Union's (EU) General Data Protection Regulation (GDPR), which uses 'explicit consent' as one legal basis around use of data, including data gathered or accessed through technological means (Publications Office of the European Union, 2016). However, it is just one legal basis – it is not a requirement that all businesses, for example, obtain consent from people before using their information (UK Information Commissioner's Office, n.d.). The UK's Information Commissioner's Office notes that 'explicit consent' is not defined in the GDPR, and then apply their own definition – this confirms the idea from the respondents that what is legal will vary across contexts. Subsequently, this implies that without a universally shared definition of consent, the question of what is legal or legitimate when framed around the issue of consent may further vary amongst contexts.

As mentioned above, legality varies in different contexts, whether jurisdictional or in relation to consent – a point well-noted by the respondents. Similarly, concerns around legal mechanisms for addressing stalkerware, identifying perpetrators and producers of stalkerware, and engaging with victims and survivors cropped up throughout the survey responses. Yet a common theme was the limited belief that the statutory sector – particularly, the police – were suited for support and action on this issue. In this regard, there is a reasonable emphasis on prioritising understanding of the current legal frameworks for future research, as well as shared definition of stalkerware specifically for use by the statutory sector in the context of legal frameworks and for law enforcement.

There is a dichotomy in the question of what type of knowledge is most needed in the field of stalkerware use in IPV, and for whom. The strongest sentiments came out around quantitative data on the prevalence of stalkerware, as well as qualitative studies of survivor/victim experiences. But simultaneously, there was an emphasis on taking more technical knowledge and understanding, such as detecting stalkerware on a device and how to remove it and transferring that knowledge to those on the front lines of stalkerware abuse – victims/survivors and support workers. This highlights the importance of avoiding singular approaches to the issue of stalkerware use in IPV and of sharing both sectoral and multidisciplinary knowledge across sectors. Overall, the experts surveyed consistently cited the importance of improving knowledge development, knowledge sharing, and engagement amongst sectors engaged in this issue.

LIMITATIONS AND CHALLENGES

There were a few key limitations common across all the studies of the present research.

The first limitation was conducting the entirety of this research only in English, a decision made due to the collective language abilities of our research team. This criterion may have excluded significant perspectives and insights from the research field. For example, some

potentially relevant publications did appear in our initial, informal searches in both Spanish and Portuguese.

Another limitation to our data collection was time. The project had a tight schedule and as such we were constrained to allocate a limited completion timeframe to the literature review, to the interview rounds, and to the survey.

We are also aware that some bias on our part may have informed important aspects of the analysis across the studies, such as literature coding and themes identified from the interviews or the inclusion of certain questions in the survey over others.

Specific to the literature review, some inclusion and exclusion criteria might have been a limitation. Restricting our search to publications released from 2010 to 2020 may mean that relevant publications beyond this timeframe were missed. However, we considered this limitation to be acceptable as the field is quite new.

Technical challenges might have represented a further limitation. A couple of survey respondents noted some technical challenges in completing it, either in open comments or through contact with us via our provided email address. This may have resulted in some data entered incorrectly on their part, thus misrepresenting their intended insights.

Across the interviews and survey, there were some limitations to our participant selection methods. For example, for the interviews, our criteria might have excluded relevant contacts working on stalkerware and IPV in fields we did not specify, or at education levels beyond those of the inclusion criteria. Snowballing contacts from our supervisor, from our literature review, and from interview participants might have provided us with a narrow participant pool that is not representative of the global community tackling stalkerware use in IPV. However, we chose a non-probabilistic and focused sampling approach because the purpose of our research was to assess the state of knowledge of a specific community, specifically that working on stalkerware and IPV.

For the surveys, the self-identification of participants is also a known form of self-selection bias and may have resulted in potential participants either selecting in when they were not our target audience or vice versa, skewing the representativeness of our results. Overall, these factors indicate that our participants, while numerous, may not be representative of the overall population of all experts in the fields of stalkerware and IPV. However, as Jarvis and Macdonald noted in their study, setting boundaries around expertise is a nebulous process given the constant fluctuation of topics, individuals, and institutions in and out of a research field, so this was to be expected.

OVERALL DISCUSSION

Current and Future Knowledge

Definitions of Stalkerware and Their Use

The most commonly used terms across all studies to refer to this phenomenon were ‘stalkerware’ and ‘spyware’. The term ‘spyware’ was referred to as a more generalised term, while stalkerware was referred to specifically in the context of IPV. However, across the studies, definitions of stalkerware provided in the literature, by interviewees, and by survey respondents varied widely. Some commonalities included frames around ‘consent’, ‘access’, ‘lack of awareness’, and ‘covertness’, but otherwise the variations underscored our earliest

insight: that this research field, while supplemented by valuable contributions from many sectors, has not produced consistent, shared knowledge.

One recent attempt to synthesise knowledge on stalkerware comes from the Coalition Against Stalkerware, as previously mentioned (see 'Study 2. Interviews'). Unlike the reflections from our studies' participants, this definition restricts stalkerware to certain types of technologies – specifically software, though on which types of devices is left undefined – and the action of monitoring. However, the emphasis on a lack of consent and lack of awareness (via notification) does echo our findings and reflects how the issue of stalkerware use in IPV can be placed into a broader context around abuses of any kind that are enabled by technology.

Recent research, current events, and emerging legislation are all circling the notion that any technology can be used for harm as much as it can be used for good. That an affected individual is made aware of these potential harms and states their willingness to be subject to that technology anyway forms a critical argument in conversations on how the statutory sector can counter potentially harmful technologies (UK Government, 2019; UK Information Commissioner's Office, n.d.).

As agreed by our survey respondents, this further supports the notion that the statutory sector might benefit most from an agreed definition of stalkerware. Definitions across issues related to IPV are critical, as noted by a representative of Women's Aid UK in commenting in 2019 on the UK Government's then-debate on draft legislation to tackle domestic abuse: 'Getting the definition right is crucial for guiding not only policies and strategies, but priorities and funding at local level and in public sector agencies, and getting that understanding of domestic abuse across all areas of the public sector that survivors might turn to for help' (UK House of Commons, 2019).

Gaps in and Future Paths for the Research Field

Our studies also revealed that in-depth knowledge about stalkerware is lacking. Across sectors, these gaps range from the user pathways that bring perpetrators to use stalkerware, to which geographic locations have stalkerware is most or least used, to what advice can best support victims. While each study surfaced some understanding of each of these elements, few pieces of knowledge had been rigorously tested, consistently observed, or widely shared. Critical data points, such as the actual prevalence of stalkerware use and the size of the stalkerware market, were still lacking.

All studies highlighted the urgent need to identify and improve anti-virus detection capabilities (sometimes linked to having a shared definition for and categorisation of stalkerware). Interview and survey respondents cited the need to produce advice and guidance for victims/survivors in a way that is actionable and scalable to other contexts. Interview and survey results strongly emphasised the necessity of centring research on survivors/victims' perspectives and experiences.

Current knowledge is clustered regionally. For example, most research activity, as identified across our studies, is currently taking place in the US followed by Australia in the literature review and the UK in the survey and interviews. Canadian researchers and professionals, despite having produced foundational literature on stalkerware and IPV were not well represented in the survey and interviews, as opposed to the literature review. These differences may be, in part, due to limitations in our study design and reach (see 'Limitations and Challenges'). The studies also revealed some knowledge silos by sector; for example, most research activity is currently coming from academia, while the statutory sector is poorly represented. This is a significant limitation of the current research field. This

idea was underscored by our studies' interview and survey participants, who stressed the value of knowledge sharing across disciplines – for example, transferring both sociological understanding of abuse victims and technical know-how between academia, support organisations and law enforcement.

A further contributing factor to these knowledge gaps is the resource scarcity within relevant sectors – in particular within the voluntary sector. Specifically, support organisations working at the frontline would benefit greatly from resources from other sectors in terms of awareness raising, technology training, and funds.

Culture as a Defining Factor

Knowledge sharing in the overall domain of IPV is also affected by two diametrically opposed cultural norms – sensationalism, particularly through news media, versus secrecy. The latter stems in part from the challenges of soliciting information from victims on stalkerware use in IPV, worsened in the context of stalkerware use by the often-covert nature of these technologies. However, higher hurdles still are the cultures of fear, victim blaming, and shaming that deter victims from coming forward and sharing their experiences.

Cultural norms are significant not only to whether victims engage with research and potential resources around stalkerware use in IPV. They are also crucial in how stalkerware itself is viewed culturally, both within research and in policy discussions or potential measures to mitigate its use.

'Legitimacy' in Culture and Law

A high number of survey respondents agreed that stalkerware technologies or their associated functions may sometimes be viewed as culturally 'legitimate'. A commonly cited example was parental control apps, with legitimacy viewed through the lens of intent. In theory at least, the legitimate intent between parental control apps is to protect (Gosh et al., 2018). Regardless, children will not always consent to their parents installing parental control apps (Ghosh et al., 2018).

The survey respondents and interviewees also described the supposed legitimacy of stalkerware technologies as a legal construct. Where legitimacy was framed as a legal issue, it was often noted that some functions of stalkerware technologies are legally allowed functions to enable in a consumer technology, and that this complicates efforts to use legislative or law enforcement mechanisms to mitigate stalkerware use. Yet, as noted by both interviewees and survey participants, 'legality' is founded in cultural contexts itself, and thus cannot be separated from conversations about a culture than enables or supports surveillance.

Normalisation of Surveillance

In particular, the studies' participants raised concerns about how stalkerware use is both supported by and itself supports a culture that normalises surveillance. Beyond government-oriented oversight for the purposes of national security, surveillance also

comes into play through cameras integrated in all of our devices, location tracking in wearables, and many other means of monitoring activity through increasingly ubiquitous technologies. This high saturation of surveillance-enabled technologies and other cultural shifts have contributed to what is called a 'surveillance society' in regions like the US (The Human Rights, Big Data and Technology Project, n.d.). In this way, the ability to monitor others has gained some cultural legitimacy and has been normalised. One example is an app like Find My Friends, which was among those cited across all studies by some literature and some participants as a type of stalkerware, despite the apparent legitimacy or normalisation of their location tracking function.

Potential Solutions and Existing Hurdles to Legislative Approaches

Seemingly, the most effective approach to take would be to simply make all stalkerware technologies or functions associated with stalkerware technologies illegal. However, survey respondents and interviewees noted multiple issues with this approach. First was that existing legislation could already be used to effect against stalkerware – but this is not happening due to lack of valuable engagement from law enforcement and the judiciary. Secondly, the transnational nature of stalkerware limits the ability to enforce legislation on technologies that are developed, sold and used across jurisdictional boundaries. Interwoven with these concerns is the question of who is targeted in such legislation and related law enforcement – for example, individuals targeting victims with these technologies versus the broader ecosystem producing or enabling production of these technologies.

On the one hand, enforcement of existing legislation might help in addressing the issue of stalkerware – although, as mentioned above, legal frameworks governing its development, distribution and use vary across national contexts. The legal analysis of stalkerware carried out by Parsons et al. (2019) specifically addresses the issue in the realm of consumer protection and data privacy within the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) and the EU's GDPR. Their account concluded that both stalkerware businesses and third-party intermediaries are accountable under both legal regimes (Parsons et al., 2019). In the Australian context, Molnar and Harkin (2019) concluded that stalkerware breaches the Australian Privacy Act. A recent legal perspective of the English context, moreover, established that the malicious use of stalkerware might be a legal offence under the Computer Misuse Act 1990, Data Protection Act 2018 and the Serious Crime Act 2015 (Brown, 2020).

The transnational nature of the issue of stalkerware use in IPV poses a challenge to addressing it through legal mechanisms. Molnar and Harkin (2019) recognised this and recommended regional pressure on some of the identified manufacturers of stalkerware, as well as the third-party intermediaries that host or facilitate the sale of stalkerware, such as Apple and Google.

From our studies we can also infer that legislation – regardless of geographical context – needs to better account for the fact that technology often enables abuses and harms that already exist, rather than create completely new issues to tackle. In this regard, legislation should place equal attention to crime occurring online as crime occurring offline. In the UK, for instance, technology-facilitated gender-based violence was entirely overlooked in the 2019 Online Harms White Paper, and the role of technology in domestic abuse is only currently being discussed within the Domestic Abuse Bill (UK Government, 2019; UK Government, 2020). Another example of this disconnect: a report by the anti-virus firm Kaspersky showed that stalkerware downloads increased by 373% from 2018 to 2019 (Kaspersky, 2019), but, as also noted in Studies 1 and 2, there is barely any evidence of

domestic abuse prosecutions. This echoes the broader trend in the literature pointing out that legislative gaps in terms of domestic violence and stalking should be closed (Molnar & Harkin, 2019; Tanczer et al., 2019), especially in view of the fact that there is a gap between what we know of the availability of stalkerware and prosecutions in this space.

Leveraging Consent and Intent in the Law

The issues of consent and intent as it relates to regulating, acting upon, and defining stalkerware are essential and at the end of the day, intrinsically legal.

One potential avenue to explore in legislating against stalkerware use is consent, which is often used to distinguish legitimate use of a technology and regulate its applications (Publications Office of the European Union, 2016). Baker (2009) stated that the role of consent in criminal law is to allow for the claim of legality of an act. Baker also stated the limits and complexities that these arguments have, namely coercion, which was also noted in the literature review and in the interviews, and the choice of irreversible harm (Baker, 2009; Molnar & Harkin, 2019). Relevant to stalkerware, Baker maintained that it is difficult to judge consent of an action whose harm can be irreversible but is not instant, and rather takes place over the long-term whereby the original point of consent struggles to account for the prolonged impact (Baker, 2009). In the context of intimate partner violence, Henry and Powell (2016) note the importance of consent in their breakdown of image-based abuse policy and law development in Australia. Following Australia's Criminal Code Amendment (Private Sexual Material) Bill 2015 the onus of removing image-based abuse, and verifying consent of images, falls on the website operator (Henry & Powell, 2016).

On the other hand, intent can be difficult to prove – even though this same framing is often a fundamental aspect of criminal law. For example, there is the question of corporate responsibility towards the actual versus intended use of a technology. The team behind *The Predator in Your Pocket* argued that ultimately it is not just the intent of the perpetrator that matters when regulating stalkerware, but also the intent of the developers who purposefully designed the technology (Parsons et al., 2019). Research carried out at Cornell Tech underlined that stalkerware is not produced or marketed accidentally, pointing to an intention which warrants inspection (Chatterjee et al., 2018). Harkin, Molnar and Vowles (2020) noted that stalkerware companies pass on the responsibility of ensuring the consent of the individual targeted with stalkerware, and third parties affected onto the customer.

By contrast, if legislators were to rely on the Coalition Against Stalkerware's definition, the scope becomes quite broad: no matter the intent of use, if a software is capable of being used without the consent of the subject to monitor, then it may still be considered stalkerware. Were future legislation to target stalkerware with this definition, this would seemingly open the doors to prosecution against a much wider array of technologies and a much broader ecosystem of perpetrators and enablers of stalkerware use in IPV.

Next Steps

In attempting to map the state of knowledge on stalkerware use in IPV, we have encountered a field even more complex than initially understood. Foundational elements of that knowledge – notably the definition of stalkerware – remain in question. Where this knowledge is not shared, researchers involved in this work agree that it should be going forward – particularly across disciplines. While some in-depth knowledge is concentrated in disciplines such as the anti-virus community and frontline support services, their knowledge

can still be improved and their efforts to mitigate stalkerware use can be vastly improved by taking up knowledge from each other's disciplines, and from others' as well. In addition, an emerging awareness, from the general public to policy makers, of potential harms from technology writ large can and should be leveraged to address the use of stalkerware in IPV. Critically, these leverage points potentially include existing legislative or law enforcement mechanisms based in well-developed framings such as consent. Future action on stalkerware use in IPV across disciplines hinges upon knowledge shared across disciplines.

Conclusion

In this research project, we observed a wide span of research and knowledge on the topic of stalkerware and IPV. Through our various queries – across published literature, of known experts, and of a broad range of researchers – we were able to identify some areas of consensus, many areas of debate and discussion, and critical issues to be addressed in future. Importantly, it is clear that existing knowledge, particularly data on the prevalence of stalkerware, in this field is quite newly developed and still limited. This remains a concern for tackling the issue from any number of angles, from legislation, to detection, to policing, to victim support.

This research did not occur in a vacuum; it was conducted amidst and alongside other, ongoing research and collaboration from both long-time experts and new entrants to this space. As mentioned previously, the Coalition Against Stalkerware – representing advocacy groups, software developers, security firms, and survivors – accomplished one of the objectives recommended from our research: agreeing on a definition of stalkerware. Across most of our studies, we observed both a collective desire and need for such a definition, so we are encouraged to see this. It is notable that in our survey, respondents felt such a definition would be most useful for the statutory sector. We hope both our insights on the mix of perspectives in defining stalkerware, plus definitions like the Coalition's, can support increased understanding and more targeted action on this issue.

As awareness and understanding is coalesced, this will better support engagement across sectors, and as with the Coalition's work, it is evident that cross-sectoral collaboration is furthering critical pieces of that shared knowledge. With regard to specific sectors and the work they still must do, the statutory and voluntary sectors stand out. From funding research (a critical component, for example, of Australia's success in producing data and developing knowledge and awareness of this issue), to developing or acting on legislation to tackle various issues in this field, to improving handling of stalkerware incidents, the heaviest scrutiny is on policy makers and law enforcement.

Concurrently, we can report anecdotally that there has been increasing awareness of the broader challenge of intimate partner violence throughout the course of our research, as it occurred amidst the 2020 COVID-19 pandemic, which has seen a reported rise in IPV and domestic violence reporting. This highlighted the importance for us of conducting such research and sharing knowledge of various tactics used in these contexts, including stalkerware.

We hope those insights can be used by a range of stakeholders to inform ongoing and future research and critical actions to root out stalkerware and its use in intimate partner violence.

References

Australian Government. (2017) *Telecommunications Act 1997*. Available from: https://www.legislation.gov.au/Details/C2017C00179 [Accessed 11 September 2020].

Australian Government. (2018) *Enhancing Online Safety Act 2015*. Available from: https://www.legislation.gov.au/Details/C2018C00356 [Accessed 11 September 2020].

Australian Government eSafety Commissioner. (2020a) *Online training for frontline workers*. Available from: https://frontlineworkers.esafety.gov.au/ [Accessed 11 September 2020].

Australian Government eSafety Commissioner. (2020b) *Online Safety Grants Program*. Available from: https://www.esafety.gov.au/about-us/what-we-do/our-programs/online-safety-grants-program [Accessed 11 September, 2020].

Baker, D. (2009) The Moral Limits of Consent as a Defense in the Criminal Law. New Criminal Law Review: *An International and Interdisciplinary Journal*. 12(1), 99-121. Available from: doi:10.1525/nclr.2009.12.1.93 [Accessed 11 September 2020].

Berreby, D. (03/03/2017) Click to agree with what? No one reads terms of service, studies confirm. *The Guardian*. Available from: https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print [Accessed 11 September 2020].

Boell, S. & Cecez-Kecmanovic, D. (2015) On being 'Systematic' in Literature Reviews in IS. *Journal of Information Technology*, 30(2), 161-173. Available from: doi:10.1057/jit.2014.26 [Accessed 11 September 2020].

Braun, V., & Clarke, V. (2008) Using thematic analysis in psychology. *Qualitative Research in Psychology*. 3 (2), 77-101. Available from: doi:10.1191/1478088706qp063oa [Accessed 11 September 2020].

Bridge, M., Hamilton, F., & O'Neill, K. (02/05/2018) Google cashes in on spy apps for stalkers following partners [Eire Region]. *The Times*. Available from: https://www.thetimes.co.uk/article/google-is-cashing-in-on-spy-apps-for-stalkers-mzx29jwj0 [Accessed 11 September 2020].

Brown, N. (11/06/2020) "How to spy on my wife's phone": an English law perspective on an article about stalkerware. *Internet, telecoms, and tech law decoded*. Available from: https://decoded.legal/blog/2020/06/how-to-spy-on-my-wifes-phone-an-english-law-perspective [Accessed 11 September 2020].

Chatterjee, R., Doerfler, P., Orgad, H., Havron, S., Palmer, J., Freed, D., Levy, K., Dell, N., McCoy, D., & Ristenpart, T. (2018) The Spyware Used in Intimate Partner Violence. *IEEE Symposium on Security and Privacy*. 441-458. Available from: doi:10.1109/SP.2018.00061 [Accessed 11 September 2020].

Chayn. (n. d.) *About Chayn*. Available from: https://chayn.co/about/ [Accessed 11 September 2020].

Chebyshev, V. (25/02/2020) Mobile malware evolution 2019. *Kaspersky Securelist*. Available from: https://securelist.com/mobile-malware-evolution-2019/96280/. [Accessed 11 September 2020].

Coalition Against Stalkerware. (2020) *What Is Stalkerware?*. Available from: https://stopstalkerware.org/what-is-stalkerware/ [Accessed 11 September 2020].

Computer Security and Privacy for Survivors of Intimate Partner Violence. (n. d.) *IPV Tech Research*. Available from: https://www.ipvtechresearch.org/research [Accessed 11 September 2020].

Cornell Tech. (03/04/2020) *Cornell Tech Clinic Helps Domestic Violence Survivors During COVID-19 Crisis*. Available from: https://tech.cornell.edu/news/cornell-tech-clinic-helps-domestic-violence-survivors-during-covid-19-crisis/ [Accessed 11 September 2020].

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2017) Digital Technologies & Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders. *Human-Computer Interaction*. 1 (46), 1-22. Available from: doi: 10.1145/3134681 [Accessed 11 September 2020].

Freed, D., Havron, S., Tseng, E., Gallardo, A., Chatterjee, R., Ristenpart, T., & Dell, N. (2019) "Is my phone hacked?" Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence. *Human-Computer Interaction*. 3(202), 1-24. Available from: 10.1145/3359304 [Accessed 11 September 2020].

Ghosh, A., Badillo-Urquiola, K., Guha, S., LaViola Jr., J., & Wisniewski, P. (2018) Safety vs. Surveillance: What Children Have to Say about Mobile Apps for Parental Control. *CHI Conference on Human Factors in Computing Systems*. 124, 1-14. Available from: doi: 10.1145/3173574.3173698 [Accessed 11 September 2020].

Grant, M. & Booth, A. (2009) A typology of reviews: an analysis of 14 review types and associated methodologies. *Health Information & Libraries Journal*, 26(2), 91-108. Available from: doi:10.1111/j.1471-1842.2009.00848.x [Accessed 11 September 2020].

Harkin, D., Molnar, A., & Vowles, E. (2020) The commodification of mobile phone surveillance: An analysis of the consumer spyware industry. *Crime Media Culture*. 16(1), 33-60. Available from: doi:10.1177/1741659018820562 [Accessed 11 September 2020].

Heartfield, R., Loukas, G., Budimir, S., Bezemskij, A., Fontaine J., Filippoupolitis, A., & Roesch, E. (2018) A taxonomy of cyber-physical threats and impact in the smart home. *Computers & Security*. 78, 398-428. Available from: 10.1016/j.cose.2018.07.011 [Accessed 11 September 2020].

Henry, N., & Powell, A. (2016) Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law. *Social & Legal Studies*. 25(4), 397-418. Available from: doi:10.1177/0964663915624273 [Accessed 11 September 2020].

The Human Rights, Big Data and Technology Project. (n. d.) *Big Data, Mass Surveillance, and The Human Rights, Big Data & Technology Project*. Available from: https://www.hrbdt.ac.uk/big-data-mass-surveillance-and-the-human-rights-big-data-technology-project/ [Accessed 11 September 2020].

Jarvis, L., & Macdonald, S. (2015) What Is Cyberterrorism? Findings From a Survey of Researchers. *Terrorism and Political Science*. 27(4), 657-678. Available from: doi: 10.1080/09546553.2013.847827 [Accessed 11 September 2020].

Johnson, M.P. (2008) *A Typology of Domestic Violence: Intimate Terrorism, Violent Resistance, and Situational Couple Violence*. Boston, Northeastern University Press. Available from: muse.jhu.edu/book/15706 [Accessed 11 September 2020].

Kaspersky. (2019) *The State of Stalkerware in 2019*. Coalition Against Stalkerware. Available from: https://media.kasperskydaily.com/wp-content/uploads/sites/92/2019/11/18053214/Kaspersky_Coalition_The-state-of-stalkerware-in-2019_ENG_fin.pdf [Accessed 11 September 2020].

Khan, K., Kunz, R., Kleijnen, J., & Antes, G. (2003) Five steps to conducting a systematic review. *Journal of the Royal Society of Medicine*. 96, 118-121. Available from: 10.1258/jrsm.96.3.118 [Accessed 11 September 2020].

Khoo, C., Roberston, K., & Deibert, R. (2019) *Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications*. Citizen Lab Report #120. Available from: https://citizenlab.ca/docs/stalkerware-legal.pdf [Accessed 11 September 2020].

Laxton, C. (2014) *Virtual World, Real Fear: Women's Aid report into online abuse, harassment and stalking*. Women's Aid. Available from: https://1q7dqy2unor827bqjls0c4rn-wpengine.netdna-ssl.com/wp-content/uploads/2015/11/Women_s_Aid_Virtual_World_Real_Fear_Feb_2014-3.pdf [Accessed 11 September 2020].

Leitão, R. (2019) Technology-Facilitated Intimate Partner Abuse: a qualitative analysis of data from online domestic abuse forums. *Human-Computer Interaction*. 00, 1-40. Available from: https://doi.org/10.1080/07370024.2019.1685883 [Accessed 11 September 2020].

Lopez-Neira, I., Patel, T., Parkin, S., Danezis, G., & Tanczer, L. (2019). 'Internet of Things': How Abuse is Getting Smarter. *Safe – The Domestic Abuse Quarterly*. 63, 22-26. Available from: doi:10.2139/ssrn.3350615 [Accessed 11 September 2020].

Molnar, A., & Harkin, D. (2019) *The Consumer Spyware Industry: An Australian-based analysis of the threats of consumer spyware*. Deakin University & ACCAN. Available from: https://accan.org.au/files/Grants/2017%20successful%20projects/Deakin%20-%20Consumer%20Spyware%20Industry%20%20-%2030Jul19%20WEB.pdf [Accessed 11 September 2020].

Nield, D. (19/07/2020) How to Check Your Devices for Stalkerware. *WIRED*. Available from: https://www.wired.com/story/how-to-check-for-stalkerware/ [Accessed 11 September 2020].

Nowell, L., Norris, J., White, D., & Moules, N. (2017) Thematic Analysis: Striving to Meet the Trustworthiness Criteria. *International Journal of Qualitative Methods*. 16 (1), 1-13. Available from: doi:10.1177/1609406917733847 [Accessed 11 September 2020].

Parsons, C., Molnar, A., Dalek, J., Knockel, J., Kenyon, M., Haselton, B., Khoo, C., & Deibert, R. (2019) *The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry*. Citizen Lab Research Report #119. Available from: https://citizenlab.ca/docs/stalkerware-holistic.pdf [Accessed 11 September 2020].

Perry, J. (2012). *Digital stalking: A guide to technology risks for victims*. Women's Aid. Version 2. Available from: https://www.womensaid.ie/assets/files/pdf/digital_stalking_guide_v2_nov_2012.pdf [Accessed 11 September 2020].

Publications Office of the European Union. (2016) *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016: on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504 [Accessed 11 September 2020].

Roundy, K., Mendelberg, P., Dell, N., McCoy, D., Nissani, D., Ristenpart, T., & Tamersoy, A. (2020) The Many Kinds of Creepware Used for Interpersonal Attacks. *IEEE Symposium on Security and Privacy*. 626-643. Available from: doi: 10.1109/SP40000.2020.00069 [Accessed 11 September 2020].

Tanczer, L., Lopez-Neira, I., Parkin, S., Patel, T., & Danezis, G. (2018) *Gender and IoT Research Report: The rise of the Internet of Things and implications for technology-facilitated abuse*. UCL. Available from: https://www.ucl.ac.uk/steapp/sites/steapp/files/giot-report.pdf [Accessed 11 September 2020].

Tseng, E., Bellini, R., McDonald, N., Danos, M., Greenstadt, R., McCoy, D., Dell, N., & Ristenpart, T. (2020) The Tools and Tactics Used in Intimate Partner Surveillance: An Analysis of Online Infidelity Forums. *29th USENIX Security Symposium*. 1892-1909. Available from: http://nixdell.com/papers/Tseng-2020-USENIX-Sec_Tools-Tactics-Intimate-Partner-Surveillance.pdf [Accessed 11 September 2020].

UK Government. (2019) *Online Harms White Paper*. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf [Accessed 11 September 2020].

UK Government. (03/03/2020) *Enhanced Domestic Abuse Bill introduced to Parliament: Ground-breaking Domestic Abuse Bill to receive First Reading in the House of Commons*. Available from: https://www.gov.uk/government/news/enhanced-domestic-abuse-bill-introduced-to-parliament [Accessed 11 September 2020].

UK Home Office. (2012) Review of the Protection from Harassment Act 1997: Improving Protection for Victims of Stalking: Summary of Consultation Responses and Conclusions. HM Home Office. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/157899/stalking-responses.pdf [Accessed 11 September 2020].

UK House of Commons. (2019) *Oral evidence: Draft Domestic Abuse Bill, HC 2075*. Available from: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-domestic-abuse-bill-committee/draft-domestic-abuse-bill/oral/99005.html [Accessed 11 September 2020].

UK Information Commissioner's Office. (n. d.) *Guide to the General Data Protection Regulation (GDPR); Lawful basis for processing*. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/ [Accessed 11 September 2020].

Wells, K., & Klosowski, T. (06/04/2020) Domestic Abusers Can Control Your Devices. Here's How to Fight Back. *New York Times Wirecutter*. Accessible from: https://www.nytimes.com/wirecutter/blog/domestic-abusers-can-control-your-devices-heres-how-to-fight-back/ [Accessed 11 September 2020].

WHO. (2018) *WHO: Addressing Violence Against Women Key achievements and priorities*. World Health Organisation. Available from: http://apps.who.int/iris/bitstream/handle/10665/275982/WHO-RHR-18.18-eng.pdf?ua=1 [Accessed 11 September 2020].

Winder, D. (08/03/2020) How to stop your smart home spying on you. *The Guardian*. Available from: https://www.theguardian.com/technology/2020/mar/08/how-to-stop-your-smart-home-spying-on-you-lightbulbs-doorbell-ring-google-assistant-alexa-privacy [Accessed 11 September, 2020].

Woodlock, D. (2017) The Abuse of Technology in Domestic Violence and Stalking. *Violence Against Women*. 23 (5), 584-602. Available from: doi:10.1177/1077801216646277 [Accessed 11 September 2020].

Appendix A. High-Relevance Texts from Literature Review

Asian News International. (27/12/2014) Use of surveillance software by abusive spouses reaches 'epidemic proportions'. Asian News International. Available from: https://in.news.yahoo.com/surveillance-software-abusive-spouses-reaches-epidemic-proportions-081227467.html [Accessed 13 September 2020].

The Argus. (08/10/2019) 'You're lucky it's just me': The case of the Australian stalker who arrived, eerily, at his ex-girlfriend's bedside. The Argus. Available from: https://search.proquest.com/docview/2312682906?accountid=14511 [Accessed 13 September 2020].

Blunden, M. (28/08/2018) Abusive partners use 'smart home' tech against hundreds of women. Evening Standard. Available from: https://www.standard.co.uk/tech/abusive-partners-use-home-technology-to-stalk-and-abuse-women-study-shows-a3921386.html [Accessed 13 September 2020].

Bridge, M., Hamilton, F., & O'Neill, K. (02/05/2018) Google cashes in on spy apps for stalkers following partners [Eire Region]. The Times. Available from: https://www.thetimes.co.uk/article/google-is-cashing-in-on-spy-apps-for-stalkers-mzx29jwj0 [Accessed 11 September 2020].

Chatterjee, R., Doerfler, P., Orgad, H., Havron, S., Palmer, J., Freed, D., Levy, K., Dell, N., McCoy, D., & Ristenpart, T. (2018) The Spyware Used in Intimate Partner Violence. IEEE Symposium on Security and Privacy. 441-458. Available from: doi:10.1109/SP.2018.00061 [Accessed 11 September 2020].

Coldewey, D. (16/08/2019) Toolkit for digital abuse could help victims protect themselves. Tech Crunch. Available from: https://techcrunch.com/2019/08/15/toolkit-for-digital-abuse-could-help-victims-protect-themselves/ [Accessed 13 September 2017].

Cox, J. (22/10/2017). Google Pushed Illegal Phone Spyware to Snoop on Your Spouse: It's malware that stalkers love, and it poses a real threat in domestic violence. Until this week, the search giant was running thousands of ads for the creepy surveillance tool. The Daily Beast. Available from: https://www.thedailybeast.com/google-pushed-illegal-phone-spyware-to-snoop-on-your-spouse [Accessed 13 September 2020].

Dudley-Nicholson, J. (24/08/2019) Google's spyware illegal. The Daily Telegraph. Available from: https://search.proquest.com/docview/2278102654?accountid=14511 [Accessed13 September 2020].

Fitzsimmons, C. (15/09/2019) Special ops squad targets domestic violence. Sun Herald. Available from: https://www.smh.com.au/technology/how-the-salvos-are-using-special-ops-to-combat-family-violence-20190913-p52qxs.html [Accessed 13 September 2020].

Flach, R. & Deslandes, S. (2019) Cyber dating abuse or proof of love? The use of apps for surveillance and control in affective-sexual relations. Cad Saude Publica. 35(1). Available from: doi: 10.1590/0102-311X00060118 [Accessed 13 September 2020].

Freed, D., Havron, S., Tseng, E., Gallardo, A., Chatterjee, R., Ristenpart, T., & Dell, N. (2019) "Is my phone hacked?" Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence. Human-Computer Interaction. 3(202), 1-24. Available from: 10.1145/3359304 [Accessed 11 September 2020].

Harkin, D., Molnar, A., & Vowles, E. (2020) The commodification of mobile phone surveillance: An analysis of the consumer spyware industry. Crime Media Culture. 16(1), 33-60. Available from: doi:10.1177/1741659018820562 [Accessed 11 September 2020].

Havron, S., Freed, D., Chatterjee, R., McCoy, D., Dell, N., & Ristenpart, T. (2019) Clinical computer security for victims of intimate partner violence. 28th USENIX Security Symposium. 105-122. Available from: https://www.usenix.org/system/files/sec19-havron.pdf [Accessed 13 September 2020].

Kaspersky. (2019) The State of Stalkerware in 2019. Coalition Against Stalkerware. Available from: https://media.kasperskydaily.com/wp-content/uploads/sites/92/2019/11/18053214/Kaspersky_Coalition_The-state-of-stalkerware-in-2019_ENG_fin.pdf [Accessed 11 September 2020].

Fraser, K. (23/09/2012) New phone spyware has alarm bells ringing. The Sunday Mail. Available at: https://www.couriermail.com.au/news/queensland/mobile-phone-spyware-has-alarm-bells-ringing/news-story/0b867125f50c9f66c1ae0f4dcf671edb [Accessed 13 September 2020].

Khoo, C., Roberston, K., & Deibert, R. (2019) Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications. Citizen Lab Report #120. Available from: https://citizenlab.ca/docs/stalkerware-legal.pdf [Accessed 11 September 2020].

Lee, K., Anderson, J. (2016) The Internet & Intimate Partner Violence: Technology Changes, Abuse Doesn't. Criminal Justice. 31(2), 28-33. Available from: https://vawnet.org/material/internet-intimate-partner-violence-technology-changes-abuse-doesnt [Accessed 13 September 2020].

Leitão, R. (2019) Technology-Facilitated Intimate Partner Abuse: a qualitative analysis of data from online domestic abuse forums. Human-Computer Interaction. 00, 1-40. Available from: https://doi.org/10.1080/07370024.2019.1685883 [Accessed 11 September 2020].

Matthews, T., O'Leary, K., Turner, A., Sleeper, M., Woelfer, J., Shelton, M., Manthorne, C., Churchill, E., & Consolvo, S. (2017) Security and Privacy Experiences and Practices of Survivors of Intimate Partner Abuse. IEEE Security & Privacy. Available from: doi:10.1109/MSP.2017.3681046 [Accessed 13 September 2020].

Meyer, J. (2012) What to Do If You Are Being Stalked, Harassed, or Spied On. Family Advocate. 35(1), 44-48. Available from: https://search.proquest.com/docview/1027613281/abstract/39BB298238BA49B2PQ/1?accountid=14511 [Accessed 13 September 2020].

Milmo, C. (26/12/2014) Abusers using spyware apps to monitor partners reaches 'epidemic proportions'. The Independent. Available from: https://www.independent.co.uk/news/uk/home-news/exclusive-abusers-using-spyware-apps-to-monitor-partners-reaches-epidemic-proportions-9945881.html [Accessed 13 September 2020].

National Network to End Domestic Violence. (2014) Technology Safety & Privacy: A Toolkit for Survivors. Available from: https://www.techsafety.org/resources-survivors [Accessed 13 September 2020].

Nilesh, C. (14/03/2018) Tools to Hack Your Phone are Getting Cheaper by the Day [Companies: Pursuit of Profit]: Digital rights organisation says Indian users need to adopt safe practices to protect their privacy. The Economic Times. Available from: https://search.proquest.com/docview/2054131444/citation/F22CBB27FE934896PQ/1?accountid=14511 [Accessed 13 September 2020].

Parsons, C., Molnar, A., Dalek, J., Knockel, J., Kenyon, M., Haselton, B., Khoo, C., & Deibert, R. (2019) The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry. Citizen Lab Research Report #119. Available from: https://citizenlab.ca/docs/stalkerware-holistic.pdf [Accessed 11 September 2020].

National Consumers League. (04/06/2014) Sen. Al Franklen Holds a Hearing on the Location Privacy Protection Act, Panel 2. Political Transcript Wire. Available from: https://search.proquest.com/docview/1532178363/citation/344B9B8109C9404BPQ/1?accountid=14511 [Accessed 13 September 2020].

Renzetti, (22/06/2019) When the stalker is your phone: It's a frightening new reality for women: Smartphones are the new frontier for stalking, and the law hasn't caught up. The Globe and Mail. Available from: https://www.theglobeandmail.com/opinion/article-when-the-stalker-is-your-phone-a-frightening-new-reality-for-women/ [Accessed 13 September 2020].

Simon, M. (04/01/2018) What To Do If Spyware Comes Up In Your Relationship. All Tech Considered. Available at: https://www.npr.org/sections/alltechconsidered/2018/01/04/556185863/what-to-do-if-spyware-comes-up-in-your-relationship?t=1600017626619 [Accessed 13 September 2020].

Roundy, K., Mendelberg, P., Dell, N., McCoy, D., Nissani, D., Ristenpart, T., & Tamersoy, A. (2020) The Many Kinds of Creepware Used for Interpersonal Attacks. IEEE Symposium on Security and Privacy. 626-643. Available from: doi: 10.1109/SP40000.2020.00069 [Accessed 11 September 2020].

Williams, R. (25/01/2015) Spyware and smartphones: how abusive men track their partners. The Guardian. Available at: https://www.theguardian.com/lifeandstyle/2015/jan/25/spyware-smartphone-abusive-men-track-partners-domestic-violence [Accessed 13 September 2020].

Appendix B. Coding for Literature Review

Relevance	Source Type	Rigour	Methodology
None	News media	Low	Investigation (journalism)
Low	PhD dissertation	Medium	General reporting (journalism)
Medium	Trade media	High	Interviews
High	Academic research publication		Legal analysis
	Private sector resource		Technical study
	Government (non-LE) publication/resource		Experiment
	Law enforcement publication/resource		Market analysis
	Advocacy/support org. publication/resource		Investigation (government)
	Independent research		Literature review
	Academic journal		Workshops
	Investigative media		Participant observation
			Case study
			Survey
			Discourse analysis
			Content analysis
			Semiological analysis

Topic	Terminology describing tech	Stakeholders	Region
Tech-facilitated abuse	Malware	Private sector (e.g. companies themselves in ecosystem)	US
Study on IPV	Stalkerware	Perpetrators	Canada
Study on stalkerware	Spyware	Survivors/victims	Australia
Discrete incidents of stalkerware use in IPV	IoT	General public	UK
Frequency of stalkerware use in IPV (general mention)	Parental control/monitoring	Policymakers	South Africa
Data on stalkerware use in IPV	Anti-virus/spyware/malware detection	Researchers	Netherlands
Detailed study of stalkerware use in IPV	Creepware	Stalkerware developers	Canada
Regulation affecting stalkerware use in IPV	Spouseware	Advocates	India
Anti-stalkerware practices	Social media/networking site	Anti-stalkerware companies	Ireland
Advice about tech-facilitated abuse in IPV	Surveillance tech/software/app	Front-line workers	Trans-national
Legal challenges related to stalkerware	Instant/text messaging	Statutory sector	Malaysia
Dual-use technology	Stalking apps		EU
Experience of survivors of tech abuse	Dual-use app		
Public opinion of tech abuse and/or stalkerware	Consumer surveillance technology		
	Tracking software/app/device		
	Keylogger software		
	Monitoring applications/software		
	GPS		
	Electronic surveillance		
	DIY spying software		
	Anti-violence applications		
	Drone		
	Nuisanceware		
	Employee monitoring apps		
	smart home security systems		
	Smartphone apps		
	Anti-theft app		
	Child monitoring		
	Online communication tools		
	Family tracking app		
	Spy app/technology		
	Phone		
	Email		

Appendix C. Interview Questions

Introduction

In your role as X, could you please tell us a bit more about the primary focus of your work?

In what region or country is your work carried out?

Following on from the previous question, could you please explain how your work intersects with the issue of stalkerware?

- Have you conducted research on the use of technology in IPV?
- Specifically, have you conducted research on the use of technologies that track location, monitor web activity, log keystrokes, or similar?
- Does your work tend to primarily focus on any of the following topics within the field of stalkerware?
    - Language used for advertising and rationalising stalkerware use
    - Functions of stalkerware apps
    - Experiences of survivors of stalkerware abuse
- If applicable:
    - Who, if anyone, has funded your work on stalkerware (e.g., research funding bodies/industry/third sector organisations)?
    - For whom, if anyone, was your work produced (e.g., research funding bodies/industry/third sector organisations)?
    - What is your primary mode of research? (e.g., technical analysis, market analysis, content analysis, experiments, surveys, interviews, workshops, field research)

How widespread is the level of awareness on the issue of stalkerware within the community/communities you work with?

Definitions and Foundations

We are aware that stalkerware is only one way to define software products and technologies used to monitor the behaviour and actions of others. To better understand the different terms used to label such concepts, could you explain what other descriptions – even in other languages – you have come across?

- For instance, are you familiar with any of the following terms? Stalkerware, spyware, spouseware, creepware, parental control apps, dual-use apps
- Can you share your definition and understanding of them?
- Do you use any of these terms more frequently than others in your work? If so, why?
- Do you use any other terms or definitions in your work?

What products or services come to your mind when you hear the term stalkerware?

What are your top three concerns when it comes to the issue of stalkerware?

What are your top three hurdles to prevent and/or mitigate the malicious usage of stalkerware in intimate partner violence settings?

It might seem odd, but can you envision any possible advantages that arise from the use of stalkerware in intimate partner violence settings? For example, does it provide useful evidence for law enforcement?

Support and Resources

What kind of resources (e.g., guidance, training, reporting tools) on the issue of stalkerware are you aware of?

- Why did you choose to mention these resources?
- What are the strengths and weaknesses of these resources?

What kind of support organisations specific to the issue of stalkerware are you aware of?

- Why did you choose to mention these organisations?
- What is your perception of these organisations?

Current Research Field

What kind of research teams or research outputs specific to the issue of stalkerware are you aware of?

- How did you come across these research teams/outputs?

© Tomás Bermudez, Maddalena Esposito, and Jay Neuner

- What is your perception of these research teams/outputs?

To the best of your knowledge, what is the research field currently doing well when it comes to stalkerware?

To the best of your knowledge, what is the research field not doing well when it comes to addressing stalkerware?

- What are gaps in the research that you feel need more attention?
- What are the issues that, to the best of your knowledge, are the most urgent to solve?
- Why do you think these issues have not been addressed yet?

What publications (if any) – e.g. from media, trades, academia, etc. – have you found most useful in carrying out research on stalkerware?

- What publications have you found to be most reliable and up to date?
- What publications have been most useful when communicating your research (if any)?

Future Research Field

From your perspective, what should further research on the topic of stalkerware carefully examine? What should these studies achieve?

Are there any potential research methods that you feel would most benefit research on the use of stalkerware (e.g., technical analysis, market analysis, content analysis, experiments, surveys, workshops, field research)?

Are there any research methods that you feel have been ineffective in your experience when carrying out research on stalkerware? What brings you to say this?

Are there any expected challenges that you might foresee arising from research in the field of stalkerware?

Other Sectors' Work

What is your experience with and perception of the voluntary sectors' response towards stalkerware (i.e., this includes non-profit charities, advocacy groups, and support networks)?

- What are they doing well when it comes to stalkerware?
- What are they not doing well when it comes to stalkerware?
- Has their response changed over time? If so, how?

What is your experience with and perception of the statutory sectors' response towards stalkerware (i.e., this includes police services, the health sector, and the judiciary)?

- What are they doing well when it comes to stalkerware?
- What are they not doing well when it comes to stalkerware?
- Has their response changed over time? If so, how?

What is your experience with and perception of the media's engagement with stalkerware?

- What are they doing well when it comes to stalkerware?
- What are they not doing well when it comes to stalkerware?
- Has their response changed over time? If so, how?

Our Research Project

What do you envision and/or hope the beneficial outcomes or our research project to be? How could we make our research project more useful to you and your community/communities?

As part of our research, we are planning to set up an online questionnaire on stalkerware to quantitatively survey self-identified researchers and experts like yourself who are working on and around the topic of technology-facilitated domestic/sexual violence and abuse, cybersecurity, and policing. In addition to the issues, we covered during this interview, are there any other survey items/questions you think we should include?

Further Pointers

Are there any other individuals or organisations you recommend we should contact for this research project?
Do you have any final questions, points, comments or concerns you would like to share with the research team?

Background Information

What participant category do you feel most aligned with?

- Academia (i.e., any academic researchers such as PhD Students, PostDocs, and faculty members employed in the higher education sector)
- Statutory Sector (i.e., any government departments, local authorities, or any other statutory body such as health, judiciary, or police representatives)
- Voluntary Sector (i.e., any voluntary and community actors from organisations such as non-profit charities, advocacy groups, and support networks)
- Tech Sector (i.e., any industry stakeholders working for private information technology services run as businesses)
- Media (i.e., any journalists and reporters who collect, write, or distribute news or other current information to the public)
- Other (if other, please specify)

If you feel comfortable answering this question, how would you describe your gender?

If you feel comfortable answering this question, would you be able to tell us how old you are?

Appendix D. Survey Questions

Consent Form

1. Please tick the box below to indicate that you consent to participate in this study and that you: have read the Participant Information Sheet and understand what the research involves; understand that your participation is voluntary and that you are free to withdraw from the task at any time, without having to give a reason, and without any consequences; and understand that you are giving the research team the right to use and make available the information you share (though not attributed to you and your organisation without further consent) in the following ways: publications in academic journals and other media; reports, online media, blogs, policy briefings; and public lectures and talks.

- o I consent

Background Information

2. How would you specify the primary focus of the workplace you are operating in?

- o Academia (i.e. any academic researchers such as PhD students, postdocs, and faculty members employed in the higher education sector)
- o Statutory sector (i.e. any government departments, local authorities, or any other statutory body such as health, judiciary, or law enforcement representatives)
- o Voluntary sector (i.e. any voluntary and community actors from organisations such as non-profit charities, advocacy groups, and support networks)
- o Tech sector (i.e. any industry stakeholders working for private information technology services run as businesses)
- o Media (i.e. any journalists and reporters who collect, write, or distribute news or other current information to the public)
- o Decline to answer
- o Other: _____

3. If you are working within academia, what best describes your disciplinary background?

- o Anthropology/Sociology
- o Economics/Business
- o Engineering/Computer science/Cybersecurity
- o Law/Criminology
- o Literature/Arts/History/Languages/Philosophy
- o Medicine/Health
- o Political science/International relations
- o Psychology
- o Social work
- o Other: _____

4. How would you describe your gender?

- o Female
- o Male
- o Nonbinary or genderqueer
- o Decline to answer
- o Prefer to self-describe: _____

5. How old are you? [single selection from 18 to 70, plus 'Decline to answer']

6. What countries or territories are you working in? [multi-selection from UK Foreign Commonwealth Office's list of approved British English-language names for countries and territories as of 5 June 2019, plus '(All)', 'Decline to answer', and 'Other']

If you selected 'Other', please share the relevant countries or territories below.

7. What countries or territories does your work cover? [multi-selection from UK Foreign Commonwealth Office's list of approved British English-language names for countries and territories as of 5 June 2019, plus '(All)', 'Decline to answer', and 'Other']

If you selected 'Other', please share the relevant countries or territories below.

Defining Stalkerware

8. Could you please share your definition of stalkerware (or write 'Decline to answer')?

9. Please indicate how frequently you use the following terms to describe the technology being used to track, monitor, stalk, and harass in intimate partner violence settings.

	Never	Rarely	Occasionally	Sometimes	Frequently	Usually	Every time	N/A
Stalkerware								
Spyware								
Spouseware								
Creepware								
Dual-use apps								
Surveillance-ware								

If you wish to provide more context, please do so below.

10. In your opinion, which of the following are important elements of stalkerware?

- o Accessing files on a device
- o Accessing the device user's personal information
- o Controlling on-device activity
- o Digital means
- o Individual (non-organisation) users
- o Key logging
- o Location tracking
- o Monitoring on-device activity
- o Restricting on-device activity
- o Targeting someone known personally by the app user
- o Don't know
- o Decline to answer

11. In your opinion, are there any important elements of stalkerware missing from the list above?

- o Yes
- o No
- o Don't know
- o Decline to answer

If you have answered the previous question with 'Yes', could you please elaborate?

12. Please indicate your level of agreement with the following statements about the categorization of stalkerware.

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree	N/A
Stalkerware is software installed on a mobile phone.								
Stalkerware is software installed on a laptop/tablet/PC.								
Stalkerware includes GPS tracking devices.								
Stalkerware includes social media.								
Stalkerware includes drones.								
Stalkerware includes smart home devices/Internet of Things devices.								

Stalkerware is only software that operates covertly.								
Stalkerware is software that operates both covertly and overtly.								
Stalkerware is legitimate and legal software that may be used maliciously.								

If you wish to provide more context, please do so below.

13. Please indicate your level of agreement with the following statements about the characteristics of stalkerware.

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree	N/A
Stalkerware is installed through physical access to a device by people who are not the primary users of that device.								
Stalkerware is software that aims to gather information surreptitiously.								
Stalkerware is primarily concerned with monitoring on-device activity.								
Stalkerware is primarily concerned with restricting on-device activity.								
There are some legitimate uses of the functions primarily associated with stalkerware, notably: monitoring on-device activity, controlling on-device activity, restricting on-device activity, or tracking device location.								

If you wish to provide more context, please do so below.

14. How important, in your opinion, is a specific and widely agreed definition of stalkerware for the following sectors?

	Not at all important	Low importance	Slightly important	Neutral	Moderately important	Very important	Extremely important	N/A
Academia								
Voluntary sector								
Statutory sector								
Tech sector								
Media								

If you wish to provide more context, please do so below.

Current Knowledge on Stalkerware

15. How would you assess your own current level of knowledge on stalkerware?

- o Poor
- o Fair
- o Good
- o Very good
- o Excellent
- o N/A

16. When did the issue of stalkerware first come to your attention? [single selection from 1995 to 2020, plus 'Decline to answer' and 'Don't know']

17. In your opinion, which countries or territories are leading the research field on stalkerware? [multi-selection from UK Foreign Commonwealth Office's list of approved British English-language names for countries and territories as of 5 June 2019, plus 'Decline to answer', 'Don't know', 'None', and 'Other']

If you selected 'Other', please share the relevant countries or territories below. You may also provide additional context on your response, if you wish to do so.

18. Which of the following products or services have you previously heard of within the context of stalkerware? [multi-selection of list of stalkerware apps, plus 'Decline to answer', 'None', and 'Other']

Android apps, Apple apps, Cerberus, Couple Tracker, Desktop Shark, Facebook, FlexiSpy, Find My Friends, Find My iPhone, Glympse, Google Maps, HelloSpy, Highster, Hoverwatch, Life360, MMGuardian, MobileSpy, Mobistealh, MonitorMinor, mSpy, Mysms, OneSpy, PhoneSheriff, RetinaX, SpyBubble, SpytoApp, Spyzie, TalkTool, TeenSafe, TheONESpy, TheTruthSpy, Trackview, Xspy, WebWatcher

If you selected 'Other', please share the relevant products or services below. You may also provide additional context on your response, if you wish to do so.

19. Please indicate your level of agreement with the following statements about gender and stalkerware use.

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree	N/A
Stalkerware has the greatest impact on people who are female.								
Stalkerware has the greatest impact on people who are male.								
Stalkerware has the greatest impact on people who are nonbinary or genderqueer.								
Stalkerware has the greatest impact on people who are transgender.								
Stalkerware has no greater impact on any gender identity than others.								

20. Please rate the importance, in your opinion, of the following identified limitations of research into stalkerware.

	Not at all important	Low importance	Slightly important	Neutral	Moderately important	Very important	Extremely important	N/A
Access to data								
Fragmented/siloed research community								
Lack of definitional consensus								
Lack of financial support/res-ources								
Lack of government collaboration with researchers								
Lack of industry collaboration with researchers								
Lack of technical knowledge								

If you wish to provide more context, please do so below.

Future Research on Stalkerware

21. Please rate the importance, in your opinion, of addressing the following potential topics of future research on stalkerware.

	Not at all important	Low importance	Slightly important	Neutral	Moderately important	Very important	Extremely important	N/A
Data on the prevalence of stalkerware use in intimate partner violence								
Document-ing stalkerware business revenue streams								

Further technical understanding of stalkerware								
Insights from survivors/ victims on their experienc-es								
Investigati-ng the presence of commercial producers of stalkerware on device app stores								
Mapping and analysis of legislation targeting or related to the use of stalkerware								
Mapping of the commercial producers and related corporate actors involved in producing stalkerware								
Understanding of how to improve frontline support								
Understan-ding the behaviours and psychology of purchasers/users of stalkerware								
Universally agreed definition of stalkerware								

If you wish to provide more context, please do so below.

21. Please rate the importance, in your opinion, of using the following research methods in future research on stalkerware.

	Not at all important	Low importance	Slightly important	Neutral	Moderately important	Very important	Extremely important	N/A
Case study								
Content analysis								
Delphi study								
Discourse analysis								
Field research								
Interviews								
Journalistic enquiry								
Literature review								
Market analysis								
Semiologi-cal analysis								
Survey								
Technical analysis								
Workshops								

If you wish to provide more context, please do so below.

21. Please rate the importance, in your opinion, of focusing on the following stakeholder groups in future research on stalkerware.

	Not at all important	Low importance	Slightly important	Neutral	Moderately important	Very importa nt	Extremely important	N/A
Perpetrators								
Victims/survivors								
Statutory sector								
Tech sector								

Voluntary sector								

If you wish to provide more context, please do so below.

Assessing the Risk of Stalkerware

24. In your opinion, have the risks associated with stalkerware changed in the last five years?
    - o Decreased
    - o Stayed the same
    - o Increased
    - o Don't know
    - o Decline to answer

If you wish to provide more context, please do so below.

25. In your opinion, will the risks associated with stalkerware change in the next five years?
    - o Decrease
    - o Stay the same
    - o Increase
    - o Don't know
    - o Decline to answer

If you wish to provide more context, please do so below.

26. Please indicate your level of concern about the following risks associated with stalkerware.

	Not at all concerned	Slightly concerned	Somewhat concerned	Moderately concerned	Extremely concerned	N/A
Economic losses						
Loss of personal data						
Loss of personal property						
Normalisation of surveillance of intimate partners						
Risk to personal mental safety						
Risk to personal physical safety						
Risk to safety of others in the same physical location as a victim/survivor						
Risk to safety of dependents						

If you wish to provide more context, please do so below.

Countering Stalkerware

27. Please rate the effectiveness, in your opinion, of the following countermeasures against stalkerware.

	Not at all effective	Slightly effective	Somewhat effective	Moderately effective	Extremely effective	N/A
Cutting revenues for stalkerware companies						
Developing and deploying on-device technical solutions to identify and report stalkerware						
Improving knowledge and effective response to stalkerware in law enforcement						
Providing frontline workers with knowledge on how to detect and act upon stalkerware						
Providing the general public with knowledge on how to detect and act upon stalkerware						
Providing victims/survivors with knowledge on how to detect and act upon stalkerware						

Raising awareness across the statutory and the voluntary sectors						
Regulating the production and/or use of stalkerware						

If you wish to provide more context, please do so below.

28. Please select, in your opinion, the top three hurdles to preventing and/or mitigating the malicious usage of stalkerware in intimate partner violence settings (at least one selection required).

- o Commercial availability of stalkerware apps
- o Lack of adequate on-device detection tools to find stalkerware on devices
- o Lack of adequate technological defences against stalkerware
- o Lack of awareness about stalkerware use in IPV among law enforcement
- o Lack of awareness about stalkerware use in IPV among policymakers
- o Lack of awareness about stalkerware use in IPV among potential victims
- o Lack of awareness of stalkerware use in IPV among law enforcement
- o Lack of relevant legislation and/or action on production of stalkerware from policymakers
- o Lack of relevant legislation and/or action on use of stalkerware from policymakers
- o Lack of sufficient consequences or accountability for use of stalkerware
- o Lack of technological skills among law enforcement to forensically analyse devices infected with stalkerware
- o Lack of urgency in addressing stalkerware production or capabilities by tech companies
- o Normalisation of surveillance in intimate relationships
- o Perceptions and approach to victims/survivors by law enforcement
- o Technological ease of publishing and/or distributing stalkerware apps
- o Decline to answer
- o Other: _____

If you wish to provide more context, please do so below.

29. Please rate the importance, in your opinion, of the following potential actions needed within the voluntary sector to address the use of stalkerware in intimate partner violence settings.

	Not at all important	Low importance	Slightly important	Neutral	Moderately important	Very important	Extremely important	N/A
Cooperating with the tech sector								
Developing guidance and toolkits for victims/ survivors								
Expanding capacity to deal with stalkerware abuse								
Increasing awareness of stalkerware use in IPV								
Allocating specific funding to stalkerware-focused programmes								
Increasing technologic-al literacy and skills								
Recruiting frontline workers with cross-cutting knowledge								

If you wish to provide more context, please do so below.

30. Please rate the importance, in your opinion, of the following potential actions needed within the statutory sector to address the use of stalkerware in intimate partner violence settings.

	Not at all important	Low importance	Slightly important	Neutral	Moderately important	Very important	Extremely important	N/A
Developing or, if existing, improving legislation targeting commercial producers of stalkerware, domestic abuse, and/or privacy								

Developing or, if existing, improving legislation targeting perpetrators of stalkerware-based IPV								
Improving overall competency in dealing with intimate partner violence and gender-based violence								
Increasing awareness across relevant entities of stalkerware use in IPV								
Increasing funding to law enforcement to aid action on stalkerware use in IPV								
Increasing funding to researchers to aid knowledge gathering on stalkerware use in IPV								
Increasing funding to voluntary sector to aid action on stalkerware use in IPV								
Increasing technological skills to forensically analyse devices infected with stalkerware among law enforcement								
Seeking out and prosecuting commercial producers of stalkerware								
Seeking out and prosecuting perpetrators of stalkerware-based IPV								

If you wish to provide more context, please do so below.

31. Please rate the importance, in your opinion, of the following potential actions needed within the tech sector to address the use of stalkerware in intimate partner violence settings.

	Not at all important	Low importance	Slightly important	Neutral	Moderately important	Very important	Extremely important	N/A
Cooperating with the voluntary sector								
Developing guidance for judiciary to aid stalkerware victims/ survivors								
Developing guidance for law enforcement to aid stalkerware victims/ survivors								
Developing guidance for potential victims/ survivors to protect against stalkerware abuse								
Developing guidance for voluntary sector to aid stalkerware victims/ survivors								
Increasing awareness of stalkerware								
Increasing development of stalkerware detection technologies								
Increasing development of technologic-al safeguards to prevent stalkerware use								
Increasing monitoring of and action against commercial producers of stalkerware within their ecosystems (e.g. app stores)								

If you wish to provide more context, please do so below.

32. Do you have any final questions, points, comments or concerns you would like to share with the research team?

33. Would you like to have the findings of this study emailed to you? If so, please provide your email address below.