TAMARA WILSON

Spying on your spouse? The inadequacy of legal protection for intimate partner victims subject to spyware and surveillance technology

Submitted for the LLB (Honours) Degree

Faculty of Law

Victoria University of Wellington

2020

Abstract

There is a growing concern among the family violence sector regarding the use of spyware and surveillance technology to harass, intimidate, stalk and coerce victims. Once a device is compromised by spyware, a person can track the GPS location of the user, access message information and in certain circumstances, have live access to the camera and microphone. The availability of such powerful instruments of surveillance is a general threat to privacy; however it is a pronounced level of danger for victims of family violence, who often rely on technology as a safety aid.

This paper examines the adequacy of existing legal remedies available to victims of spyware and surveillance technology. It concludes that the technology faces definitional barriers and ultimately falls within a legislative gap. Additionally, systematic biases and attitudes limit victims' ability to seek support. New Zealand's laws dealing with surveillance are in danger of falling behind those of other comparable countries such as Australia and the United Kingdom. The paper concludes by recommending a range of measures that relate to public legal education, enhanced law enforcement responses and law reform.

Keywords: *family violence, technology-facilitated abuse, spyware, cyber-stalking*

Table of Contents

I Introduction

> Violence often has a purpose, so that he can maintain power over her, to stop her from doing things that he does not want her to do, to make her do certain things, or to punish her for not meeting his demands. Technology provides a new way for these men to monitor her movements, control her social word, harass and limit her freedom by keeping her afraid.[1]

Family violence is a devastating issue which has affected New Zealand for generations.[2] While the motivations of family violence perpetrators have remained consistent, the tools in which they have access to have drastically changed in the modern age. As technology exponentially advances, users face growing threats to security and privacy in the form of direct monitoring programmes – victims of family violence disproportionately carry these risks.

New Zealand's Women's Refuge has acknowledged an "increasingly disturbing trend of perpetrators using smartphones, software and apps to track and stalk women".[3] Their advocates report "feeling frustrated with the [legislative] barriers clients face when accessing safety mechanisms".[4] This paper assesses these barriers and examines the adequacy of existing legal remedies available to victims of spyware and surveillance technology.

As intimate partner surveillance occurs during a relationship and after,[5] an "intimate partner" in this paper includes all current relationships such as partners, de facto relationships and spouses. "Intimate partners" will also be used interchangeably with "victims." Although not all technology-facilitated surveillance occurs in the confines of family violence, emerging research suggests the technology is becoming increasingly prevalent in intimate relationships.[6] Therefore, there is a compelling case for New Zealand's legislative framework to be reviewed against other jurisdictions to ensure it provides parity of protection in the offline and technology-facilitated world.

---

[1] Clem Bastow "Digital abuse is the new frontier of domestic violence" *Daily Life* (online ed, Australia, 16 February 2014).
[2] Genevieve Leigh Coleman "Are you Really Okay? An Easier and More Effective Solution for Obtaining Protection Orders" (LLB (Hons) Dissertation, University of Otago, 2016) at 3.
[3] Scoop "Seeking Safety Online" (press release, 17 May 2016).
[4] Natalie Thorburn and Ang Jury "Relentless, not Romantic: Intimate Partner Stalking in Aotearoa New Zealand" (2 December 2019) Women's Refuge <www.womensrefuge.org.nz> at 11.
[5] Delanie Woodlock "Technology-facilitated Stalking: Findings and Recommendations from the SmartSafe Project" (2014) Domestic Violence Resource Centre Victoria <www.dvrcv.org.au> at 12.
[6] Delanie Woodlock "The Abuse of Technology in Domestic Violence and Stalking" (2017) 23(5) VAW 584.

This introduction forms Part I of the paper. Part II explains the nature of spyware and surveillance technology. It will examine how perpetrators are increasingly turning to software to terrorise victims, with computer and smartphone applications offering fertile ground for surveillance strategies to become embedded with little risk or exposure.[7]

Part III is a review of key sections of current legislation in New Zealand. It analyses whether legislation sufficiently protects family violence victims of spyware and surveillance technology. Protection orders and criminal charges are the leading and most permanent remedy for family violence victims.[8] Thus, both remedies are assessed.

Part IV concludes that despite a growing international concern for spyware and surveillance technology in family violence, New Zealand's current legislation fails to deal with the problem adequately. A range of potential amendments and measures are considered, including a new offence which may better encapsulate the ongoing, controlling and coercive nature of intimate partner violence. Legislative amendments, however, without an effort to improve social understanding will only have a symbolic effect.

II Spyware and Surveillance Technology

Surveillance technologies are dual-use devices (such as a home security camera or smartphone) repurposed to monitor and observe a person's actions or communications in an ongoing way.[9] Where a smartphone or computer is used, the technology is often repurposed using spyware – a type of software available on the application store, developed to secretly observe a person's activities.[10] Spyware apps are available in New Zealand.[11] Installing spyware on victim's computers or smartphones is one of the most common methods of surveillance.[12] The software does not verify consent from the person being monitored and fails to make the user of the device aware the spyware is being used. Once downloaded, the software offers extensive

---

[7] Danielle Keats Citron "Spying Inc" (2015) 72 Washington and Lee L Rev 1243 at 1251.
[8] Coleman, above n 2, at 1.
[9] Law Commission *Invasions of Privacy: Penalties and Remedies: Review of the Law of Privacy Stage 3* (NZLC IP14, 2009) at 181.
[10] Adam Molnar and Diarmaid Harkin "The Consumer Spyware Industry: An Australian-based analysis of the threats of consumer spyware" (2019) Australian Communications Consumer Action Network (ACCAN) <www.accan.org.au> at 3.
[11] Ian Steward "I spy with my little app" *Stuff* (online ed, New Zealand, 08 September 2013).
[12] Cynthia Fraser and others "The New Age of Stalking: Technological Implications for Stalking" (2010) 61(4) Juv & Fam Ct J 39 at 45.

powers of surveillance to the operator and provides continuous access to information that would not otherwise be shared.

To install the software requires at least temporary physical access to the device or knowledge of the device's passwords – both of which are common in relationships. If access to a device is limited, spyware can be installed remotely. An example is the spyware app, Loverspy. Purchasers of the app send a "menu" to victims in an email. Unknown to the victims, once opening the email, Loverspy is surreptitiously installed.

Spyware and surveillance technology offer a range of capabilities which afford dramatic control and power of an individual's life. This paper will refer to four invasive capabilities of surveillance over a person.

A Visual surveillance

Typical spyware applications enable an operator to remotely command the victim's device to send live pictures and videos from the target device. Repurposed nanny or home security cameras can be used to monitor victims' daily activities and interactions.

B Audio surveillance

Targeted devices of spyware allow an operator to record or listen in real-time to outgoing or incoming phone calls. One spyware provider, FlexiSpy, enables the operator to turn the victim's device into an "audio bug" and listen in on the phone's surroundings to hear "what's really going on behind closed doors."[13]

C Tracking surveillance

Global positioning systems (GPS) use satellite signals to fix the location of a radio receiver.[14] GPS capabilities are integrated into most smartphones, for example, Find My iPhone on Apple products. Spyware can enable this geolocation data to be transmitted from the target device to the operator, allowing the location and movements of its user to be identified at all times. Spyware to transmit GPS data was used by an abusive partner in Canada, who installed the

[13] Molnar and Harkin, above n 10, at 5.
[14] Law Commission (NZLC IP14, 2009), above n 9, at 190.

software on his intimate partner's smartphone.[15] Using the data, he determined her location, where he then assaulted her.

D Data surveillance

Spyware can capture data information by intercepting emails and text messages or requesting periodic screenshots from the victim's device.[16] In a Canadian case, *Shoshi v Vuksani,* spyware enabled an abusive partner access to his ex-partner's contact information which was kept hidden for safety concerns.[17] Another common feature of spyware is keystroke technology. It records a device's keystrokes and transmits the data to the operator. Any deleted searches or messages are logged and recorded.

III Intimate partner violence and spyware and surveillance technology

A The Nature of Family Violence

In practice, non-violent family violence is a pattern of systematic behaviour that establishes dominance over another person through intimidation, isolation or fear-inducing threats of violence – termed "coercive control".[18] Patterns of coercive behaviour are recognised as key aspects of family violence in New Zealand.[19]

Perpetrators will go to great lengths to maintain power and control over their victims. Adding to the already epidemic rates of family violence, spyware and surveillance technology provide new tools to further stalk, control and monitor victims. Stark argues that stalking is the most prevalent form of surveillance used in coercive control. It conveys the perpetrator's omnipotence and presence.[20] Spyware isolates a person, deprives them of independence and thus regulates their behaviour.

---

[15] "Petaluma Man Arrested For Stalking Woman" *CBS Local* (online ed, San Francisco, 13 November 2013).
[16] Molnar and Harkin, above n 10, at 5.
[17] *Shoshi v Vuksani* 2013 ONCJ 459.
[18] Melissa E Dichter and others "Coercive Control in Intimate Partner Violence: Relationship with Women's Experience of Violence, Use of Violence and Danger" (2011) 8(5) Psychol Violence 596.
[19] Ministry of Justice *Strengthening New Zealand's Legislative response to family violence: A Public Discussion Document* (25 August 2015) at 19.
[20] Evan Stark "Looking beyond domestic violence: Policing coercive control" (2012) 12 Journal of Police Crisis Negotiations 199 at 214.

Spyware and surveillance technology abuse is part of a broader web of cyber-violence and technology-facilitated abuse. This branch of violence also includes communication technology and image-based abuse. The former involves harassing an intimate partner through excessive calls, texts or social media and the latter through sexual revenge images.[21] Whilst equally dangerous, these behaviours fall outside of the scope of this paper. Spyware and surveillance technology in intimate partner violence is referred to in the literature as intimate partner stalking or cyberstalking. This paper will use the terms interchangeably.

Intimate partner stalking is not a new phenomenon. Previously, perpetrators typically used physical acts to exert power, such as measuring mileage of car odometers or physical following.[22] Technological advancement assists perpetrators to escalate and amplify typical methods to eradicate stalking and overcome spatial boundaries. Being kept under surveillance leaves victims feeling trapped as if they are unable to completely escape their partner's presence, for they know where the victim will be at any time.[23] Being spied on may appear minor, especially when no threats are made. In the context of intimate relationships, however, the harm is unique. The parties know each other well, and the perpetrator knows how to terrify and induce fear in the victim.[24] Therefore, when an abusive intimate partner knows every level of detail about the victim's life, it can be disturbing and frightening.

Spyware and surveillance technology is commonly used covertly without the victim's knowledge or consent. Often victims only become suspicious of surveillance when their partner appears to know more than they should. In other circumstances, a perpetrator may use spyware overtly to openly intimate and induce fear. Stark asserts that overt behaviour is a tactic men use to intimidate.[25] Perpetrators are often motivated by a sense of ownership and control and believe they are righteous in their actions.[26] A perpetrator who utilises spyware and surveillance technology may never inflict physical violence because their omnipresence and knowledge become their power.

---

[21] Heather Douglas, Bridget A Harris and Molly Dragiewicz "Technology-facilitated Domestic and Family Violence: Women's Experiences" (2019) 59 Brit J Criminology 551.
[22] Cynthia Khoo, Kate Robertson and Ronald Deibert "Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing and Selling Smartphone Spyware and Stalkerware Applications" (June 2019) Citizen Lab Canada <www.citizenlab.ca>.
[23] Jonathan Clough *Principles of Cybercrime* (2nd ed, Cambridge University Press, Cambridge, 2015) at 448.
[24] Fraser and others, above n 12, at 49.
[25] Stark, above n 20.
[26] Thorburn and Jury, above n 4, at 13.

Technology is both a weapon and a shield in violent relationships. The internet is often used as a safety aid and support network when escaping a violent relationship. However, the alternative digital landscape of spyware may preclude a victim from effecting any kind of escape from the relationship. Most family violence websites provide untraceable forums, but keystroke loggers and screenshot software may expose a victim's exit strategy. Alternatively, when overt, it may provide a deterrent for victims considering leaving. In an Australian case, *R v Gittany,* Gittany installed spyware on his fiancé, Harnum's, smartphone and surveillance cameras throughout their apartment without her knowledge.[27] The technology was used to monitor her movements and "effectively spy on her private communications".[28] Harnum was preparing to leave the relationship. Gittany became aware of her escape plan by secretly reading her messages. Upon the revelation of her plans, Gittany murdered Harnum by pushing her from their 15th-floor balcony apartment.

B Prevalence in New Zealand

Family violence is increasingly recognised as one of New Zealand's most significant social problems. The 2015 *New Zealand Crime and Safety Survey (NZCASS)* found that 76 per cent of family violence incidents are unreported to police.[29] Yet, between 2000 - 2011 New Zealand experienced the highest rate of intimate partner violence than any other OECD country.[30] The 2018 *NZCASS* confirmed psychological abuse is the most common under-reported type of harm, but New Zealanders suffer from psychological abuse at "about the same rate" as they experience physical assault.[31]

Population-based stalking statistics in New Zealand are rare. Internationally, women are overwhelmingly the victims in intimate partner stalking.[32] One in every six women experience

---

[27] *R v Gittany (No 4)* [2013] NSWSC 1737.
[28] At [227] per McCullum J.
[29] New Zealand Family Violence Clearinghouse "Data Summaries 2015: Snapshot" (2015) <www.nzfvc.org.nz>.
[30] Denise Wilson and others "Becoming Better Helpers: Rethinking language to move beyond simplistic responses to women experiencing intimate partner violence" (2015) 11 Police Quarterly 25 at 26.
[31] New Zealand Family Violence Clearinghouse "Cycle 2 Key Findings" (2018) <www.nzfvc.org.nz>.
[32] Michele C Black and others "The National Intimate Partner and Sexual Violence Survey 2010 Summary Report" (2011) National Sexual Violence Resource Center <www.nsvrc.org>.

stalking in their lifetime.[33] Men are the main perpetrators of stalking.[34] Stalking is most often perpetrated by intimate or former intimate partners.[35]

Measurement of cyber-stalking prevalence is even more challenging to determine. Electronic surveillance is often covert, difficult to detect and relies on the self-report of specific online behaviours. Statistics on technology-facilitated abuse remains in their infancy, with many studies being anecdotal experiences which collapse communication technology and surveillance technology into one category.

New Zealand does not have a specific stalking or cyber-stalking criminal offence. Instead, the behaviour is classified according to an appropriate offence category. Consequently, statistics about the use of technology to stalk in New Zealand are likely to be underestimated. The Women's Refuge has acknowledged an "increasingly disturbing trend of perpetrators using smartphones, software and apps to track and stalk women" in New Zealand.[36] The age demographic of victims vary, but those who grow up with technology (ages 16-35) unsurprisingly report much higher rates of victimisation through digital means.[37]

Abuse of surveillance technology in the context of intimate partner violence is widely documented in Australia, Canada and the United Kingdom. In Canada, accusations of covert electronic surveillance in the context of family violence are "frequent".[38] American domestic violence agencies have also reflected a significant concern about the use of technology. A survey reported that sixty per cent of their clients had their partners break into their computer to monitor their activities, thirty one per cent installed spyware and fifty per cent of victims were tracked via GPS and other means.[39]

Although statistics based in New Zealand are rare, it is evident spyware and surveillance technology are a prominent feature in intimate partner violence internationally. Given the

---

[33] Black and others, above n 32.
[34] TK Logan "Research of Partner Stalking: Putting the Pieces Together" (2010) <www.ncjrs.gov>.
[35] TK Logan and Robert Walker "Toward a deeper understanding of the harms caused by partner stalking" (2010) 25(4) Violence Vict 440.
[36] Scoop, above n 3.
[37] Thorburn and Jury, above n 4, at 67.
[38] Ron Foster and Lianne Cihlar "Technology and Family Law Hearings " (2015) 5(1) Western Journal of Legal Studies 1 at 3.
[39] Brenda Baddam "Technology and it's danger to domestic violence victims: how did he find me?" (2017) 28 Alb Law J 73 at 20.

ubiquitous presence of technology and New Zealand's alarming rate of family violence, it is reasonable to conclude the behaviour is prevalent in New Zealand.

C Unique Challenges of Spyware and Surveillance Technology

1 Dual-use

Spyware has legitimate, benevolent uses. Many applications are advertised for monitoring children's behaviour and device use. However, regardless of the software's advertised purpose, there is nothing to prevent users from repurposing the functions for harmful practices. The National Network to End Domestic Violence explained:[40]

> Some developers try to mask the nefarious intentions by mentioning child safety ... but their true focus is obvious when they reiterate on every page how their products are completely hidden.

Some spyware vendors make clear stealth surveillance of intimate partners is a crucial purpose and advertise the software to "easily spy on your spouse".[41]

2 Covert

A core selling point of spyware is its covert nature. Users are assured when downloading the applications "don't worry! The software is invisible to the target user. He/she will never come to know they are being monitored."[42] Spyware is not a virus. Subsequently, it is undetected by antivirus software and tough to remove.[43]

---

[40] "Senate Bill Would Ban Stalking Apps and Save Women's Lives" (4 June 2014) The National Network to End Domestic Violence <www.nnedv.org>.
[41] Citron, above n 7, at 1247.
[42] "Top 5 Apps to Spy On Your Spouse Android Phone" Mobie Spy <www.mobiespy.com>.
[43] Daniel Garrie, Alan Blakley and Matthew Armstrong "The Legal Status of Spyware" (2006) 59(1) Fed Comm LJ 157 at 162.

3 Attitudes

Forms of cyber-violence are often downplayed and minimised as it appears less severe and distinct from other forms of abuse.[44] Often these systematic biases and attitudes create additional barriers that limit a victim's abilities to seek support.

Cyber-stalking may involve no physical contact. Consequently, it is misconceived as more benign than physical stalking, despite research showing cyber-stalking incites similar feelings of distress, anxiety, and helplessness as traditional (physical) stalking.[45]

Police and members in the community perceive stranger stalking as more problematic, intrusive and dangerous than stalking pursued by an intimate partner.[46] This perception is concerning because intimate partners are more likely to perpetrate physical violence against the victim.[47]

Many victims report their concerns of controlling behaviour were relegated to a narrative of "romantic difficulty" and therefore somewhat acceptable.[48] This flattering pursuit schema contributes to further perceptions of victim-blaming. Strategies that aim to prevent cyber-stalking are targeted at the victim's personal conduct and behaviour. For example, victims are told to "delete apps, shut off GPS, stay off social media" and change their personal digital routines.[49] Victims are advised to change *their* behaviour in order to avoid abuse. It should be clear the behaviour is a deliberate action of the perpetrator. The focus should be on holding perpetrators accountable, not advising victims to forsake their digital life.

---

[44] Bridget Harris and Delanie Woodlock "Digital Coercive Control: Insights from Two Landmark Domestic Violence Studies" (2019) 59(3) Brit J Criminology 530.
[45] Joanne D Worsley and others "Victims' Voices: Understanding the Emotional Impact of Cyberstalking and Individuals' Coping Responses" (2017) 7(2) SAGE Open 1.
[46] Bronwyn McKeon, Troy E McEwan and Stefan Luebbers "'It's Not Really Stalking If You Know the Person': Measuring Community Attitudes That Normalize, Justify and Minimise Stalking" (2015) 22(2) Psychiatry, Psychology and Law 291.
[47] McEwan and others "Violence in stalking situations" (2009) 39(9) Psychological Medicine 1469.
[48] Thorburn and Jury, above n 4, at 15.
[49] Hadeel Al-Alosi "Cyber Violence: Digital Abuse in the Context of Domestic Violence" (2017) 40(4) UNSW Law Journal 1573 at 1599.

D Impact

Privacy is not only a significant social value but also one that the law should protect.[50] Privacy refers to "a state of personal exclusion from involvement with or the attention of others".[51] The Law Commission encompasses privacy as a multifaceted concept. It includes "the right to be left alone" conducive to autonomy and security as a principle which allows people to create boundaries free of disturbance.[52] Spyware and surveillance technology undermine physical, behavioural and informational privacy. The unsolicited and constant nature of the technology violates a person's power to prevent interference and control to what extent information is made available. Tracking features detract a victim's right to locational and spatial privacy and undermine the expectation of anonymity. Despite the intimate nature of relationships, victims remain a right to privacy as an essential and indispensable value in modern civilisation.

Cyber-stalking pursued by an intimate partner results in significant emotional, social and psychological harm, even after the stalking has ended.[53] The Australian *SmartSafe* study reported that 84 per cent of intimate partner surveillance victims suffered mental health and well-being problems such as post-traumatic stress disorder, anxiety or depression.[54]

Intimate partner stalking is closely associated with and frequently escalates to physical and sexual violence.[55] Perhaps most alarming, as *R v Gittany* illustrated, is that stalking is an indicator or precursor behaviour to intimate partner homicide.[56] The most frequent types of intimate stalking behaviours preceding attempted or actual homicides include "following or spying and keeping the victim under surveillance".[57]

---

[50] Law Commission *Privacy Concepts and Issues: Review of the Law of Privacy Stage 1* (NZLC SP19, 2008) at 11.
[51] *Hosking v Runting* [2005] 1 NZLR 1 (CA) at [264].
[52] Law Commission (NZLC SP19, 2008), above n 49, at 32.
[53] Woodlock "Technology-facilitated Stalking: Findings and Recommendations from the SmartSafe Project", above n 5, at 13.
[54] At 25.
[55] Mindy Mechanic, Terri Weaver and Patricia Resick "Intimate Partner Violence and Stalking Behaviour: Exploration of Patterns and Correlates in a Sample of Acutely Battered Women" (2000) 15(1) Violence Vict 55.
[56] Judith McFarlane and others "Stalking and Intimate Partner Femicide" (1999) 3(4) Homicide Studies 300.
[57] McFarlane and others, above n 55, at 311.

Victims are justifiably terrified when their intimate partners keep them under surveillance. They are the most dangerous, the most determined, and the most likely to murder the victim. It is therefore crucial the behaviours are taken seriously.

IV Legislative Provisions

Evidently, the use of spyware and surveillance technology is an issue of growing concern. Given the technology's inherent dangers, invasive capabilities and documented association with intimate partner violence, there is a compelling case for a review of New Zealand's legislative framework. The following analysis will examine how the law may respond to protect intimate partner victims of spyware and surveillance. Such technology has not yet been closely considered in the New Zealand legal system; thus, the analysis will draw on comparable jurisdictions.

A Protection and Restraining Orders

Civil protection orders were developed as a legal response to addressing patterns of harm that are not limited to physical violence.[58] When in force, they protect the applicant from further harm by imposing several conditions the respondent must obey. The following analysis considers whether an order can be obtained against harm caused by spyware and surveillance technology. It concludes that spyware and surveillance technology are difficult to fit within current statutory definitions.

1 Family Violence Act 2018

Where violence is inflicted against a victim by a person whom the victim is, or has been, in a family relationship with, the victim will be directed to the Family Violence Act (FVA). The FVA provides a clear and unequivocal condemnation that *all* forms of family violence are unacceptable.[59] The FVA enables victims to obtain protection orders as a preventative tool against family violence.[60]

---

[58] Julia Tolmie "Coercive control: To criminalize or not to criminalize?" (2018) 18(1) Criminology & Criminal Justice 50 at 50.
[59] Section 4(a).
[60] Section 3(1)(a)-(c).

The crucial concept for obtaining a protection order is that of "family violence". An applicant must show on the balance of probabilities the respondent is currently inflicting "family violence" or has done so in the past. Family violence can be physical, sexual or psychological, but the common denominator of all the behaviours is the exertion of power and control by the offender.[61]

The Domestic Violence Act 1995, the statutory predecessor to the FVA was "not proving effective."[62] Thus, the FVA replaced the Domestic Violence Act and aimed to modernise the legislative understanding of family violence. Yet, no reference is made to forms of technology-facilitated abuse outside the scope of digital-communications. The definition of family violence now includes "coercive or controlling behaviour". The inclusion is meant to "make it clear" as to what is intended in the definition of psychological abuse, yet the FVA omits to define the term.[63] The omission may mean opportunities to intervene are being missed because the significance of each episode is underestimated.

The precise meaning of psychological abuse is left unaddressed by the FVA, but is "the type of behaviour that is difficult to describe, report, prosecute and generally guard against".[64] Section 11(1)(b) provides non-exhaustive illustrations of psychological abuse, such as "intimidation" or "harassment". Examples of harassment and intimidation in the Act include watching, loitering near and following the person.[65] These provisions suggest the respondent must have the victim under physical surveillance. Such descriptions are not applicable to digital surveillance such as monitoring electronic communications.[66]

Comparatively, Queensland and South Australia's definition of family violence includes "unauthorised surveillance".[67] Queensland's Act lists examples of "unauthorised surveillance" as "unreasonable monitoring of activities or interpersonal associations", "using a GPS device to track a person's movements" and "reading a person's SMS messages".[68]

---

[61] *Adult Relationships: Family Violence* (online ed, Thomson Reuters) at [FV9.01(1)].
[62] *Adult Relationships: Family Violence,* above n 59, at [FVIntro.01].
[63] *Adult Relationships: Family Violence,* above n 59, at [FV11.01].
[64] *Tyler v Tyler* [2014] NZFC 5173 at [50] per Judge Flatley.
[65] Section 11(1)(a)(b)(i)-(iii).
[66] Clough, above n 23, at 450.
[67] See generally Domestic and Family Violence Protection Act 2012 (Qld), s 8(2)(h) and Intervention Orders (Prevention of Abuse) Act 2009 (SA), s 8(4)(k).
[68] Domestic and Family Violence Protection Act (Qld), s 8(5).

Assuming an applicant can prove digital surveillance amounts to psychological abuse, the Family Court must furthermore be satisfied the respondent has or is inflicting family violence.[69]

When granted, the protection order contains standard conditions such as prohibiting the respondent engaging in behaviour which amounts to any form of family violence.[70] Protection orders are, therefore, crucial to stopping cyber-stalking behaviours. Their effectiveness, however, relies on a clear message that all forms of technology-facilitated abuse are a breach of legislation.[71]

It should be noted applying for a protection order is a civil, not criminal proceeding. Although a breach of a protection order is a criminal offence,[72] the issuing of a protection order does not necessarily lead to the perpetrator being held accountable for their actions. Some conduct such as physical or sexual assault may constitute a criminal offence but the New Zealand Government has shied away from criminalising psychological abuse. This is likely because the criminal law "typically responds to single incidents" and psychological harm often comprises years of cumulative harm.[73]

The FVA also enables granting of Police Safety Orders (PSO).[74] The orders give immediate short-term protection to victims at risk by removing the perpetrator from the home for a period of time. PSO are used where police are concerned there is a risk of family violence, but there may be insufficient evidence, or they do not consider it necessary to press charges. A person served a PSO cannot harass, stalk, threaten or intimidate the protected person for up to 10 days.[75] Unlike a protection order, granting a PSO does not involve the judiciary, and breach of a PSO is not a criminal offence.

---

[69] Section 79.
[70] Section 90.
[71] Al-Alosi, above n 48, at 1599.
[72] Section 112.
[73] Ministry of Justice, above n 19, at 31.
[74] Section 28.
[75] "Police Safety Orders" New Zealand Police <www.police.govt.nz>.

The FVA provides tailored protection for victims of family violence. Omitting apparent reference to modern intimate partner violence utilised by spyware and surveillance technology fails to give effect to the Act's statutory purpose and potentially leaves victims unable to access safety mechanisms.

2 The Harassment Act 1997

The Harassment Act is designed to provide further protection to victims of harassment who cannot be brought within the framework of the Family Violence Act. The Act makes the most serious forms of harassment criminal and empowers the District Court to grant restraining orders.[76] A person in a "family relationship", such as an intimate partner may not apply for a restraining order.[77] Nevertheless, it is worthy of examining any disparities in obtaining legal protection from spyware and surveillance harm for a stranger versus an intimate partner.

Harassment is defined vaguely, reflecting the difficulty in framing legislation to be wide enough to include all possible situations.[78] Harassment consists of a "pattern of behaviour" directed against another person, that includes doing any of the "specified acts" to the other person.

(a) Pattern of behaviour

A key feature of harassment is that the complainant must establish a pattern of behaviour. Prior to a 2015 amendment, a "pattern of behaviour" was limited to two separate occasions over twelve months. Such a narrow interpretation would mean a single act of continuous surveillance could not qualify as harassment. The Act now includes a broader definition of the harasser doing a specified act on one occasion that is "one continuing act carried out over any period".[79] Although aimed at digital communications such as posting a harassing comment online, a single continuous act of surveillance would likely qualify as a pattern of behaviour. This view is supported by Australian precedent, where a "course of conduct" which includes

[76] Section 16.
[77] Section 9.
[78] Jane Mountfort "The Civil Provisions of the Harassment Act 1997: A Worrying Area of Legislation?" (2001) 32 VUWLR 999 at 1000.
[79] Harassment Act, s 3(b).

surveillance, "may comprise conduct which includes keeping the victim under surveillance for a single protracted period of time".[80]

(b) Specified Act

The Harassment Act was enacted to remedy a perceived gap in the law relating to stalking.[81] Despite its origins and purpose, the current scope of harassment does not align with the range of behaviours that are considered stalking in the modern digital age.

Section 4(1)(a)-(e) provides a non-exhaustive list of "specified acts" of harassment. These include watching, loitering near, following, stopping or accosting a person. Similarly to the Family Violence Act, the provisions suggest the respondent must be engaged in physical surveillance methods.[82] No reference is made to instrumentalising tracking or monitoring applications, placing a GPS tracker on a victim's car or intercepting calls as a "specified act". Instead, a court would need to hold that digital surveillance is tantamount to "watching" or "following". The view of the Law Commission is that these acts "are probably not covered" within s 4(1)(a)-(e).[83]

Comparatively, the Protection from Harassment Act 1997 in England and Wales uses a similar phrase "course of conduct" but provides a specific reference to digital surveillance. The Act includes "monitoring the use by a person of the internet, email, or any other form of electronic communication" and "watching or spying on a person."[84]

Legislation in the Australian state of Victoria has also anticipated the use of spyware. The legislation's extensive list provides examples directly relevant to the digital context:[85]

> (bb) causing an unauthorised computer function … in a computer owned or used by

[80] *Gunes v Pearson* and *Tunc v Pearson* (1996) 89 A Crim r 297, 306.
[81] Mountfort, above n 76, at 999.
[82] Law Commission (NZLC IP14, 2009), above n 9, at 211.
[83] Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC R113, 2010) at 67.
[84] Protection from Harassment Act 1997 (UK), s 2A(3)(d).
[85] Crimes Act 1958 (Vic), s 21A.

the victim or any other person;
(bc) tracking the victim's or any other persons use of the internet or of email or other electronic communications;
…
(f) keeping the victim or any other person under surveillance.

New Zealand's Harassment Act does not explicitly account for the availability to digitally and remotely spy on a victim. The Act does, however, provide a catch-all provision designed to catch "unusual" acts:[86]

4 Meaning of specified act

…

(f) acting in any other way –

(i) that causes that person (person A) to fear for his or her safety; and
(ii) that would cause a reasonable person in person A's particular circumstances to fear for his or her safety.

The catch-all provision ensures flexibility to capture methods of harassment which evolve with technology. A complainant who is subject to surveillance may be able to satisfy the elements of s 4(1)(f) but will be subject to further qualifications of proving fear subjectively and objectively. In other words, the qualifications in s 4(1)(f)(i)-(ii) do not apply to the activities outlined in paragraphs s 4(1)(a)-(e).

The restrictions may prove unjust in the context of surveillance. On a literal reading, a victim who is physically kept under surveillance (i.e. where the act will fall within s (4)(1)(a)) will not need to prove the physical watching causes them to fear for their safety. Paradoxically, a victim who is being kept digitally under surveillance will be subject to further qualifications reliant on the measuring of suffering by the victim.

It is arguable whether the two methods of stalking are distinct enough in their harm to justify one requiring a further threshold than the other. The Colorado Court of Appeal is of the opinion

[86] *Brown v Sperling* [2012] DCR 753 at [19] per Judge Harvey.

that there is no significant difference between physically engaging in surveillance as opposed to digitally.[87] For example, using a GPS device is designed to achieve the same result as physical stalking.

In the context of cyber-stalking and s 4(1)(f), Judge Harvey is of the opinion that in order to succeed in proving fear it would "likely… [be] necessary to prove that the cyberstalker could carry out his or her threats."[88] To prove this may be a barrier to an intimate partner when using the provision for criminal harassment. Often surveillance is a form of control, not coupled with threats.

Part 3 of the Act provides the District Court power to grant a restraining order if the order is necessary for the protection of the applicant.[89] Breaching a restraining order is a criminal offence punishable by a maximum term of six months imprisonment[90] – a lesser term than that of the Family Violence Act. Unlike the high threshold in the Family Violence Act, the Harassment Act only requires the behaviour is causing or threatens to cause distress to the applicant or a reasonable person in the applicant's circumstances.[91]

B The relationship between the Family Violence Act and Harassment Act

The Harassment Act is "legislation [that] serves an analogous purpose" to the Family Violence Act.[92] Yet, in light of the requirement of proving psychological abuse, an intimate partner victim may find it difficult for identical acts to qualify as "family violence" than an applicant qualifying "harassment".[93] Potter J noted harassment in the Harassment Act is not as limited as it is in the Family Violence Act to psychological abuse. It "is a concept that has a meaning more embracing and more benign than violence under the [Family] Violence Act".[94] Thus, the Harassment Act "takes up where the family violence legislation leaves off".[95] The maximum

[87] *Colorado v Sullivan* 53 P 3d 1181 (Colo Ct App 2001).
[88] *Brown v Sperling*, above n 84, at [31].
[89] Harassment Act, s 16.
[90] Harassment Act, s25.
[91] Harassment Act, s 16.
[92] *M v M* [2005] NZHC 971 at [22] per Miller J.
[93] Ruby King "Digital Domestic Violence: Are Victims of Intimate Partner Cyber Harassment Sufficiently Protected by New Zealand's Current Legislation?" (2017) VUWLR 48(2) 29.
[94] *Beadle v Allen* [2000] NZFLR 639 at [35] and [40].
[95] Bill Atkin *Family Law Service (NZ) – Family Violence: Harassment* (online ed, LexisNexis) at [7.656].

term of punishment for a breach of a protection order is more severe than a breach of a restraining order; however, victims seeking a protection order are subject to a far more restrictive criteria than that of the counterpart legislation available for those not in a "family relationship" with the perpetrator. Protection orders are "the main way the family violence laws try to protect victims of family violence ... from future violence and abuse".[96] Yet they can only be obtained if there has been psychological abuse, suggesting a serious level of conduct. Restraining orders, available through the Harassment Act, require behaviour that causes distress. They are expansive enough to cover innocuous behaviour, allowing the law to intervene at a much lower level of harassment.[97]

C Criminal Law

The criminal law plays an essential role in emphasising what family violence behaviours society deems unacceptable. However, criminal law responds to single incidents; thus, it cannot always respond effectively to the ongoing pattern of coercive abuse which often characterises family violence.

Consider the following example: Person A purchases spyware and installs the software on his ex-wife's (person B's) computer and smartphone, without her knowledge or consent. Person A uses the software to:

(a) listen to B's oral communications;
(b) read B's digital communications; and
(c) activate B's camera and track B's location.

The following analysis examines potential barriers that may arise when prosecuting person A using the computer misuse offences in the Crimes Act 1961 or criminal harassment in the Harassment Act 1997.

(a) Listening and intercepting

The use of devices to intercept and listen to communications is governed by Part 9A of the Crimes Act. It is an offence to intentionally intercept any private communication by means of

[96] Community Law "*Protections Against Family Violence: An overview"* Community Law <www.communitylaw.org.nz>
[97] Mountfort, above n 76.

an "interception device".[98] The initial offence criminalised the use of a "listening device" but in 2003 was substituted with "interception device". Judge Harvey explains this change is directed to include electronic communications such as emails.[99] There has been no reported decision in New Zealand concerning whether spyware constitutes an interception device, but as an electronic software, it would likely be considered one. "Interception device" is defined widely and includes "any other device that is used or capable of being used to intercept a private communication". In the United States, the creator of a spyware program was charged with manufacturing an "interception device".[100]

Assuming spyware will therefore constitute an interception device, the elements of the offence may be satisfied only where person A uses spyware to listen to phone calls or read messages *as they occur* on person B's device. Section 216B(1) emphasises a controlling temporal aspect. The surreptitious interception of stored, historic private communications will not fall within the definition of "intercept". To "intercept" a private communication means to "hear, listen to, record, monitor, acquire, or receive the communication either while it is taking place or while it is in transit".[101] Therefore, person A's liability under this offence is limited to real-time and suggests the interception must be instantaneous – recorded, read or monitored on their journey from the sender to the recipient. Person A's future listening to person B's voicemail messages or reading of messages after they have been delivered cannot be considered an interception because the communication is no longer in transit.[102]

The offence fails to address the recording of voicemails, historic communications or the use of keystroke loggers before messages are sent. Instead, the monitoring of person B's electronic information after they were delivered may fall within Part 10 of the Crimes Act.

(b) Monitoring data

Part 10 of the Crimes Act prohibits crimes involving computers. Whether the application of the offences would extend to a smartphone depends on the interpretation of "computer", which

---

[98] Section 216B(1).
[99] David Harvey *Internet.Law.nz*: *Selected Issues* (2nd ed, LexisNexis, Wellington, 2005) at 242.
[100] Larry J Siegel *Criminology* (11th ed, Cengage Learning, United States of America, 2012) at 533.
[101] Crimes Act, s 216A(1).
[102] *R v Hooker* HC Wellington CRI-2005-091-2882, 20 October 2006 at [30].

is not defined within the Act. Australia, Canada and the United Kingdom similarly have left the term to be interpreted by the courts according to its ordinary usage. The deliberate absence of a definition recognises that technology is "rapidly advancing and any definition would quickly become obsolete."[103] Modern smartphones have the same processing powers as a computer, and the view of Judge Harvey is that a mobile phone could be classed as a computer.[104] Similarly, the Supreme Court of New Zealand has described cell phones as "mini-computers."[105]

Access and authority (or lack thereof) is a key element of the offences under ss 249, 250 and 252 of the Crimes Act. Defined widely, "access" includes to instruct, communicate with and receive data from. "Communicate with" could include using a smartphone to pass information to and from the computer system.[106] Therefore, "access" "likely includes the use of a virus, spyware or other malware to receive info" such as a keystroke logger.[107]

If the accessing of person B's computer system is dishonest and results in person A obtaining an advantage or benefit or causes loss to person B, person A will be found liable under s 249. Advantage or benefit has a wide meaning and is not limited to financial gain. It can include passwords or data.[108]

Under s 250(2), liability is established where a person intentionally or recklessly and without authority damages, deletes, modifies or impairs any data or software in a computer system. Damages, deletes or modifies refers to the sense of interfering with the data on it or disrupting its ability to function properly.[109] Person A's use of spyware technology would likely be a violation of this offence because spyware software is designed to "infiltrate or damage" a computer system.[110] Prior to the enactment of the computer misuse offences, spyware

---

[103] Law Commission *Computer Misuse* (NZLC R54, 1999) at 6.
[104] Harvey, above n 96, at 210.
[105] *Dotcom v Attorney General* [2014] NZSC 199, [2015] 1 NZLR 745 at [189].
[106] Harvey, above n 96, at 292.
[107] Wayne Rumbles (ed) *Electronic Business and Technology Law (NZ)* (online ed, LexisNexis) at [11.2.1].
[108] Harvey, above n 96, at 303.
[109] Amy Corkey "A 13-Year Analysis of the "Crime Involving Computers" Provisions of the Crimes Act 1961" (LLB (Hons) Dissertation, University of Otago, 2016) at 57.
[110] Department of the Prime Minister and Cabinet *National Plan to Address Cyber Crime 2015* (2015) <www.connectsmart.govt.nz> at 16.

downloaded on to a computer was held to cause "damage", suggesting that spyware may be considered damage for the purposes of s 250(2).[111]

Section 252(1) criminalises intentionally accessing (directly or indirectly) a computer system without authorisation, where the perpetrator knows they lack authorisation or are reckless as to the fact. The offence is yet to be applied to spyware, but the linkages to the elements of unauthorised access and spyware are obvious. Spyware – which can be downloaded directly or indirectly and is designed to gain surreptitious access to a device – is arguably targeted by this law. Prima facie, when person A reads and monitors person B's data through surreptitiously installed spyware, person A gains unauthorised access to a computer system and therefore may be found liable under s 252(1).[112]

Section 251 criminalises the possession of software that is intended to be used in the commission of an offence. Spyware applications are designed to enable an operator to gain unauthorised access and in some circumstances, interfere with data on that device. As such, person A's possession of spyware software may satisfy the elements of this offence.

Consider the following alternative example. A husband (person C) wants to monitor his wife's (person D's) daily activities. Person C purchases his wife a new smartphone and computer and installs spyware on the phone before he gives it to her. The spyware enables the husband to access similar functions as the first example, such as listening to the wife's oral communications, reading digital communications and tracking her location. The application of the aforementioned computer misuse offences to this example, where person C and person D are both authorised users because they have shared access or jointly own it, are limited.

Firstly, shared access to each other's computers and smartphones may engage problems regarding consent. For example, the interception and computer misuse offences do not apply in the former where the person intercepting is a party to the private communication, and in the latter when the person is authorised to do so. A person with express or implied consent is a party to the private communication.[113] Effective consent cannot be coerced and it cannot be

[111] *R v Garrett* [2001] DCR 955 at [100].
[112] Bianca Mueller "Criminal Liability for mobile phone spying in NZ" (31 January 2014) New Zealand Law Society LawTalk <www.lawsociety.org.nz>.
[113] Crimes Act, s 216A(3).

assumed that sharing access to devices is consent or authorisation to intercept *all* private communications a perpetrator can surreptitiously access. However, courts will need to consider further contextual circumstances in intimate relationships to address this issue.[114]

Secondly, the view of the Law Commission is that the computer misuse offences would *not* apply because the devices are under the perpetrators (person C's) ownership and control.[115]

Nevertheless, the offences may apply to spyware installed on an ex-partner or stranger's device as illustrated by the first example, where issues of shared ownership and control are not present.

(c) Watching, visual recording, locating and tracking

There is no criminal offence in New Zealand which prohibits the use of spyware or surveillance technology to record or monitor private activity, unless it falls within the definition of an intimate visual recording.[116] Thus, where spyware is used to activate person B's web camera remotely, and the video does not breach a reasonable expectation of privacy nor are intimate in nature, the recording will attract no new liability. This outcome would be the same if a repurposed home security camera were utilised.

Unlike in some Australian states,[117] New Zealand does not have an offence prohibiting the domestic use of location and tracking devices.

The installation of spyware will likely be a punishable offence where a perpetrator installs spyware on a device belonging to a stranger, or an ex-partner. Where intimate partners are in a relationship which gives rise to circumstances of shared ownership or access (such as marriage) they are presented with a legal grey area of laws. This gap between the application of the offences to those in an intimate relationship who share ownership to those who do not share ownership is distressing. The Women's Refuge reports a higher percentage of intimate partners

---

[114] Khoo, Robertson and Deibert, above n 22, at 26.
[115] Law Commission (NZLC IP14 2009), above n 9, at 232.
[116] Crimes Act, s 216H.
[117] See generally Surveillance Devices Act 2007 (NSW), Surveillance Devices Act 1999 (Vic), Surveillance Devices Act 1998 (WA).

are subject to monitoring, tracking and surveillance technology *during* the relationship, as opposed to after.[118]

(d) Criminal Harassment

Where the behaviour qualifies as "harassment" under the civil regime, it will be considered criminal where the offender intends to cause the person harassed to fear for their safety or has knowledge that the harassment is likely to cause the person to fear for their safety.[119] Criminal harassment carries a maximum term of imprisonment of two years.[120]

A person in a "family relationship" is not excluded from prosecuting an offender through criminal harassment but proving the impact on the victim may be a barrier for intimate partners. In intimate relationships, the behaviour may only be disruptive or create feelings of distrust and loss of autonomy. A perpetrator may not intend for their partner to fear for their safety, especially when surveillance is covert, and no threats are made.

Surveillance conducted in isolation, which is unknown to a victim may fail to satisfy the fault element of intention and impact on the victim.[121] If a victim is unaware, then it can arguably have no impact on him or her. This argument – that a person could not be harassed by surveillance of which she was unaware – was put forward by the defendant in an American case, *H.E.S v J.C.S.*[122] The plaintiff and defendant were ex-partners living in the same house but different rooms. The plaintiff found a small surveillance camera hidden in her bedroom. The Appellate Division held the defendant's actions did not constitute harassment. The offence required repeatedly committing acts with the purpose of alarming or seriously annoying the person. The defendant did not intend for her to find the camera hence the element was not satisfied.[123]

---

[118] Thorburn and Jury, above n 4, at 71.
[119] Harassment Act, s 8(1).
[120] Harassment Act, s 8(2).
[121] Clough, above n 23, at 387.
[122] *HES v JCS* 815 A.2d 405 (2003).
[123] But see the appeal – *HES v JCS,* 175 NJ 309 (SC NJ 2003). The New Jersey Supreme Court rejected these arguments when viewed in the totality of the circumstances. In addition to the camera, the defendant physically followed her places, stole items from her bedroom and threatened to kill her. When considered all together, there was sufficient evidence of conduct which could amount to harassment and stalking.

V Possible Legislative Amendments

New Zealand's legislation regulating the relationship between spyware, surveillance and family violence is patchy and lacks coherence. The view of the Law Commission is that surveillance is not comprehensively covered by any of the current modes of enforcement mentioned in this paper.[124]

The behaviours associated with spyware and surveillance technology face legislative barriers and ultimately fall within a legislative gap. The current legislation has struggled to adapt with technology-facilitated family violence without imposing additional unnecessary obstacles. Advances in technology are making surveillance more widespread, so the need to fill the gap in this area of law becomes more urgent.[125] The abovementioned legislation would benefit from explicit clarification to represent a better transparent mechanism.

Legislative reform is recommended because it is one of the key ways by which the government seeks to change behaviour and outcomes for society.[126] Legislative reform will ensure New Zealand's legal tools more effectively protect victims and hold perpetrators to account by removing definitional barriers to reduce impunity and to clearly open avenues for redress.

Legislative change, however, without an effort to improve social understanding will only have a symbolic effect. The lack of understanding about what constitutes stalking behaviour in the modern age, underlying gender inequalities and deeply entrenched patriarchal beliefs are also barriers responsible for victims' experiences being invalidated, minimised or dismissed.[127] Thus, alongside legislative amendments, action should be taken to improve societal education and to enhance law enforcement responses. Without sufficient understanding of how technology is misused by intimate partner stalkers victims are left without the justice they deserve.[128]

---

[124] Law Commission (NZLC IP14, 2009), above n 9, at 119.
[125] Law Commission (NZLC IP14, 2009), above n 9, at 119.
[126] "Legislation Guidelines: 2018 edition" (2018) Legislation Design and Advisory Committee <www.ldac.org.nz>.
[127] See Jenny Korkodeilou *Victims of Stalking: Case Studies of Invisible Harms* (Palgrave Macmillan, London, 2020) at 135.
[128] Fraser and others, above n 12, at 39.

A Tracking offence

There is currently no offence which covers the use of tracking devices as a surveillance device. GPS and tracking devices produce more information than physically following a person. When covert, they do not allow for the person being tracked to take protective measures and "genuinely threaten the safety of a person when done by an abusive partner".[129] The Law Commission recognises that the use of tracking devices to track people without their consent is a "sufficiently serious interference with privacy, autonomy and security, and it should generally be prohibited."[130]

Criminal law remedies play an important censuring function. A criminal offence *to knowingly install, use or maintain a tracking device to monitor a person without their consen*t should be enacted. Similar offences exist in Australian states which prohibit the use of devices for data or optical surveillance, listening and tracking.[131] The offence has been used to successfully prosecute offenders who installed a tracking device as a surveillance method in the context of intimate partners and family violence.[132]

B Harassment Act

There is a need for consistency between offline and technology-facilitated stalking and for the Harassment Act to better respond to other forms of harassment in the digital context. Despite being amended in 2015, the non-exhaustive specified acts listed in the legislation need regular attention. Currently, a court must rule digital surveillance is tantamount to "watching" or "following" or the applicant must prove further subjective and objective elements reliant on fear suffered. New Zealand's Harassment Act should be amended to recognise harassment in the modern digital world outside the scope of digital communications.

Two specified acts should be included in s 4(1). The first is *keeping a person under surveillance.* This act will be aimed at perpetrators who repurpose technology for surveillance

---

[129] Law Commission (NZLC R113, 2010), above n 81, at 38.
[130] Law Commission (NZLC R113, 2010), above n 81, at 38.
[131] See generally Surveillance Devices Act 2007 (NSW), Surveillance Devices Act 1999 (Vic), Surveillance Devices Act 1998 (WA).
[132] *Musgrove v Millard* [2012] WASC 60.

means. The Law Commission supports this view.[133] The second act is *causing an unauthorised computer function in a computer owned or used by the victim or any other person.* This act may be wide enough to encapsulate spyware installed on smartphones or computers without facing the barriers of joint ownership prevalent in the aforementioned computer misuse offences.

C Family Violence Act

In response to the Women's Refuge's concerns about intimate partner stalking in New Zealand, Jan Logie stated the recent family violence reform provisions could cater to victims:[134]

> [Those changes] have made it clear that family violence can be psychological as well as physical, it can manifest as a pattern of behaviour over time, and coercive control is a component of family violence.

New Zealand's legal definition of family violence now alludes to "controlling and coercive behaviour" but omits apparent reference to methods of digitally perpetrated stalking. The purpose of including coercive control is to provide the "judiciary with greater direction of what is considered [to be] family violence".[135] However, such cases will not appear in front of the judiciary if victims and law enforcement continue to operate under the misconception that using spyware and surveillance technology is not a stalking behaviour worthy of seeking protection from. Victims can be hesitant to describe their experiences as there is often confusion about what behaviours fit into the definition of stalking.[136] Sending a clear, unambiguous message that stalking is illegal in all forms is vital and "influential to the victim seeking help."[137]

An amendment should be made to the Family Violence Act 2018 as follows:

11 Meaning of psychological abuse

(1) Psychological abuse includes—

---

[133] Law Commission (NZLC R113, 2010), above n 81, at 67.
[134] Wilhelmina Shrimpton "Calls for better protection for women being stalked by an ex-partner" *Newshub* (online ed, Auckland, 14 October 2019).
[135] Ministry of Justice, above n 19.
[136] Woodlock "Technology-facilitated Stalking: Findings and Recommendations from the SmartSafe Project", above n 5, at 13.
[137] Thorburn and Jury, above n 4, at 129.

…

(b) intimidation or harassment (for example, all or any of the following behaviour that is intimidation or harassment:

…

(iv) *monitoring the movement or communications of the person using electronic means.*

The above amendment will give full effect to the Act's statutory purpose of condemning *all* forms of family violence. It will bring New Zealand's legislative response to family violence in line with other common law jurisdictions such as individual Australian states which recognise cyber-stalking as a form of family violence.[138]

D A criminal offence of coercive control?

In 2015, England and Wales created a criminal offence of controlling or coercive behaviour in an intimate or family relationship:[139]

(1) A person (A) commits an offence [of coercive control] if—

(a) A repeatedly or continuously engages in behaviour towards another person (B) that is controlling or coercive,
(b) At the time of the behaviour, A and B are personally connected,
(c) The behaviour has a serious effect on B, and
(d) A knows or ought to know that the behaviour will have a serious effect on B.

The offence intends to criminalise behaviours "that stop short of serious physical violence, but amount to extreme emotional abuse."[140] It carries a maximum penalty of five years imprisonment. One of the behaviours in the Statutory Guidance to the offence include "monitoring a person via online communication tools or using spyware".[141]

---

[138] Domestic and Family Violence Protection Act 2012 (Qld), s 8(2)(h) and Intervention Orders (Prevention of Abuse) Act 2009 (SA), s 8(4)(k).
[139] Serious Crime Act 2015 (UK), s 76.
[140] "UK to criminalise coercive, controlling and psychological abuse" (20 January 2015) New Zealand Family Violence Clearinghouse <www.nzfvc.org.nz>.
[141] Crown Prosecution Service (UK) "Controlling or Coercive Behaviour in an Intimate or Family Relationship – Legal Guidance, Domestic Abuse" (30 June 2017) CPS <www.cps.gov.uk>.

During the family violence legislative overhaul, the New Zealand Government declined to create offences for emotional and psychological abuse. The then Prime Minister John Key stated the offence was not proving as successful as intended.[142] Since then, the reported coercive control incidents in England and Wales have doubled in one year.[143]

New Zealand does not have a criminal law counterpart in the Crimes Act for non-physical violence, nor is it necessary for spyware and surveillance harm. Creating new offences should be cautioned against, especially if those laws will only be "superficially or symbolically attractive".[144] Successful prosecution will rely heavily on victim testimony and police understanding and the concept of coercive control may be minimised if the offence is not successfully used in cases where there is no physical violence.[145]

Instead, current legislation should be amended to greater accommodate non-violent harm. The Harassment Act reform would allow victims of spyware and surveillance harm to rely on the two-step criminalisation of those behaviours under the offence of criminal harassment. The notable difference between the offences is the effect it must have on the victim. Coercive control requires a lower threshold of causing a serious effect. Person B must either fear violence will be used against them or suffer serious alarm or distress, which has a substantial adverse effect on their day-to-day activities.[146] Criminal harassment, on the other hand, requires the applicant or a reasonable person in the applicant's place to fear for their safety. Safety, however, is not limited to physical. It includes a person's mental well-being.[147] A lower threshold may be easier to prove, but a lower standard risks over-criminalisation and ineffective reactive law-making.

The aforementioned amendments will better enhance the current framework, enabling victims to quickly obtain protection by clear symbolic recognition the behaviour is prohibited. Spyware

---

[142] Stacey Kirk "Strangulation, coercion to marry and family violence to be new crimes with tough sentences – Govt" *Stuff* (online ed, Wellington, 13 September 2016).
[143] Gabriella Swerling "Coercive control incidents double in a year, as campaigners warn domestic abuse 'remains at epidemic levels'" *The Telegraph* (online ed, United Kingdom, 25 November 2019).
[144] Heather Douglas "Do we need an offence of coercive control?" (2018) 5 PrecedentAULA 144.
[145] Tolmie, above n 57, at 59.
[146] Serious Crime Act 2015 (UK), s 76(4)(b).
[147] Harassment Act 1997, s 2.

and surveillance technology are recognised as stalking behaviours and should be adequately legally recognised, without being subject to further requirements than its counterpart physical stalking behaviour.

VI Conclusion

While New Zealand has taken the initiative in protecting victims of cyber-bullying and image-based abuse, the rise of consumer spyware is creating a unique challenge for the family violence sector. The use of spyware and surveillance technology in relationships is unique and a powerful tool for a batterer. The tactics capitalise on the perpetrator's knowledge of their relationship to control, intimidate and stalk their victims. The behaviour is correlated to the intensity of victims' fear and to likelihood of severe violence and homicide. It must therefore be recognised and sanctioned robustly by all agencies as a harmful form of family violence, absent of victim-blaming strategies. The application of the computer misuse criminal offences are uncertain and yet to be tested in shared ownership contexts and current legislative definitions in are inapt to deal with spyware and surveillance technology. To ensure victims can access the justice they deserve, it is proposed provisions of the Crimes Act, Family Violence Act and Harassment Act are amended. This will ensure parity of protection in the offline and technology-facilitated world. Reform must also be systemic – legislative tools are not a stand-alone remedy which will provide victims with any kind of panacea.

Word count

The text of this paper (excluding table of contents, footnotes, and bibliography) comprises approximately 7,999 words.

Bibliography

A Cases

1 New Zealand

Beadle v Allen [2000] NZFLR 639.

Brown v Sperling [2012] DCR 753.

Dotcom v Attorney General [2014] NZSC 199, [2015 1 NZLR 745.

M v M [2005] NZHC 971.

R v Garrett [2001] DCR 955.

R v Hooker HC Wellington CRI-2005-091-2882, 20 October 2006.

Surrey v Surrey [2010] 2 NZLR 581 (CA).

Tyler v Tyler [2014] NZFC 5173.

2 Australia

R v Gittany (No 4) [2013] NSWSC 1737.

Bancroft v Lindsay [2016] FCCA 1236

Gunes v Pearson and *Tunc v Pearson* (1996) 89 A Crim R 297.

Musgrove v Millard [2012] WASC 60.

3 United States of America

HES v JCS 175 NJ 309 (SC NJ 2003).

4 Canada

Shoshi v Vuksani 2013 ONCJ 459.

B Legislation

1 New Zealand

Crimes Act 1961.

Family Violence Act 2018.

Harassment Act 1997.

2 Australia

Crimes Act 1958 (Vic)

Domestic and Family Violence Protection Act 2012 (Qld).

Intervention Orders (Prevention of Abuse) Act 2009 (SA).
Restraining Orders Act 1997 (WA).
Surveillance Devices Act 1998 (WA).
Surveillance Devices Act 1999 (Vic).
Surveillance Devices Act 2007 (NSW).

3 United Kingdom

Protection from Harassment Act 1997.
Serious Crime Act 2015.

C Books

David Harvey *Internet.Law.nz: Selected Issues* (2nd ed, LexisNexis, Wellington, 2005).
Jenny Korkodeilou *Victims of Stalking: Case Studies of Invisible Harms* (Palgrave Macmillan, London, 2020)
Jonathan Clough, *Principles of Cybercrime* (2nd ed, Cambridge University Press, Cambridge 2015).
Larry J. Siegel *Criminology* (11th ed, Cengage Learning, United States of America, 2012).
Yee Fen Lin *Cyberspace Law: Commentaries and Materials* (2nd ed, Oxford University Press, Sydney, 2007).

D Journal Articles

Brenda Baddam "Technology and it's danger to domestic violence victims: how did he find me?" (2017) 28 Alb Law J 73.
Brett Eterovic-Soric and others, "Stalking the stalkers – detecting and deterring stalking behaviours using technology: a review" (2017) Computers and Security 70 278.
Bridget Harris and Delanie Woodlock "Digital Coercive Control: Insights from Two Landmark Domestic Violence Studies" (2019) 59(3) 530.
Bronwyn McKeon, Troy E McEwan and Stefan Luebbers "'It's Not Really Stalking If You Know the Person': Measuring Community Attitudes That Normalize, Justify and Minimise Stalking" (2015) 22(2) Psychiatry, Psychology and Law 291.
Cynthia Fraser and others "The New Age of Stalking: Technological Implications for Stalking" (2010) 61(4) Juv & Fam Ct J 39.
Daniel Garrie, Alan Blakley and Matthew Armstrong "The Legal Status of Spyware" (2006) 59(1) Fed Comm LJ 157.

Danielle Keats Citron “Spying Inc” (2015) 72 Wash & Lee L Rev 1243.

Delanie Woodlock and others, “Technology as a Weapon in Domestic Violence: Responding to Digital Coercive Control” (2020) Australian Social Work 73(3) 368.

Diarmaid Harkin and Adam Molnar “Operating-system Design and Its Implications for Victims of Family Violence: The comparative Threat of Smart Phone Spyware for Android Versus iPhone Users” (2020) Violence Against Women 00(0) 1.

Evan Stark “Looking beyond domestic violence: Policing coercive control” (2012) 12 Journal of Police Crisis Negotiations 199.

Hadeel Al-Alosi “Cyber Violence: Digital Abuse in the Context of Domestic Violence” (2017) 40(4) UNSW Law Journal 1573.

Heather Douglas “Do we need an offence of coercive control?” (2018) 5 PrecedentAULA 144.

Heather Douglas and Mark Burdon, “Legal Responses to Non-Consensual Smartphone Recordings” (2018) 41(1) UNSW 1.

Heather Douglas, Bridget A Harris and Molly Dragiewicz “Technology-facilitated Domestic and Family Violence: Women’s Experiences” (2019) 59 Brit J Criminology 551.

Jane Mountfort “The Civil Provisions of the Harassment Act 1997: A Worrying Area of Legislation? (2001) 32 VUWLR 999.

Joanne D Worsley and others “Victims’ Voices: Understanding the Emotional Impact of Cyberstalking and Individuals’ Coping Responses” (2017) 7(2) SAGE Open 1.

Judith McFarlane and others “Intimate Partner Stalking and Femicide: Urgent Implications for Women’s Safety” (2002) 20(12) Behavioural Sciences and the Law 12.

Julia Tolmie “Coercive control: To criminalize or not to criminalize?” (2018) 18(1) Criminology & Criminal Justice 50.

McEwan and others “Violence in stalking situations” (2009) 39(9) Psychological Medicine 1469.

Melissa E. Dichter and others “Coercive Control in Intimate Partner Violence: Relationship with Women’s Experience of Violence, Use of Violence and Danger” (2011) 8(5) Psychol Violence 596.

Mindy Mechanic, Terri Weaver and Patricia Resick “Intimate Partner Violence and Stalking Behaviour: Exploration of Patterns and Correlates in a Sample of Acutely Battered Women” (2000) 15(1) Violence Vict 55.

Ron Foster and Lianne Cihlar “Technology and Family Law Hearings” (2015) 5(1) Western Journal of Legal Studies 1.

Ruby King "Digital Domestic Violence: Are Victims of Intimate Partner Cyber Harassment Sufficiently Protected by New Zealand's Current Legislation?" (2017) VUWLR 48(2) 29.
T K Logan and Robert Walker "Toward a deeper understanding of the harms caused by partner stalking" (2010) 25(4) Violence and Victims 440.

E Parliamentary and Government Materials

Department of the Prime Minister and Cabinet *National Plan to Address Cyber Crime 2015* (2015) <www.connectsmart.govt.nz>.
Law Commission *Computer Misuse* (NZLC R54, 1999).
Law Commission *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy Stage 3* (NZLC R113, 2010).
Law Commission *Invasions of Privacy: Penalties and Remedies: Review of the Law of Privacy Stage 3* (NZLC IP14, 2009).
Law Commission *Privacy Concepts and Issues: Review of the Law of Privacy Stage 1* (NZLC SP19, 2008).
Ministry of Justice *Strengthening New Zealand's Legislative Response to Family Violence: A Public Discussion Document* (25 August 2015).

F Dissertations

Amy Corkey "A 13-Year Analysis of the 'Crime Involving Computers' Provisions of the Crimes Act 1961" (LLB (Hons) Dissertation, University of Otago, 2016).
Genevieve Leigh Coleman "Are you Really Okay? An Easier and More Effective Solution for Obtaining Protection Orders" (LLB (Hons) Dissertation, University of Otago, 2016).

G Internet resources

"Petaluma Man Arrested For Stalking Woman" *CBS Local* (online ed, San Francisco, 13 November 2013).
Adam Molnar, Diarmaid Harkin "The Consumer Spyware Industry: An Australian-based analysis of the threats of consumer spyware" (2019) Australian Communications Consumer Action Network (ACCAN) <www.accan.org.au>.
Adult Relationships: Family Violence (online ed, Thomson Reuters)
Bianca Mueller "Criminal Liability for mobile phone spying in NZ" (31 January 2014) New Zealand Law Society LawTalk <www.lawsociety.org.nz>.
Bill Atkin *Family Law Service (NZ) – Family Violence: Harassment* (online ed, LexisNexis)

Clem Bastow "Digital abuse is the new frontier of domestic violence" *Daily Life* (online ed, Australia, 16 February 2014).

Community Law "*Protections Against Family Violence: An overview"* Community Law <www.communitylaw.org.nz>.

Crown Prosecution Service (UK) "Controlling or Coercive Behaviour in an Intimate or Family Relationship – Legal Guidance, Domestic Abuse" (30 June 2017) CPS <www.cps.gov.uk>.

Cynthia Khoo, Kate Robertson and Ronald Deibert "Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing and Selling Smartphone Spyware and Stalkerware Applications" (June 2019) Citizen Lab Canada <www.citizenlab.com>.

Delanie Woodlock "Technology-facilitated Stalking: Findings and Recommendations from the SmartSafe Project (2013) Domestic Violence Resource Centre Victoria <www.dvrcv.org.au>.

Gabriella Swerling "Coercive control incidents double in a year, as campaigners warn domestic abuse 'remains at epidemic levels'" *The Telegraph* (online ed, United Kingdom, 25 November 2019).

Michele C Black and others "The National Intimate Partner and Sexual Violence Survey 2010 Summary Report (2011) National Sexual Violence Resource Center <www.nsvrc.org>.

Natalie Thorburn, Ang Jury "Relentless, not Romantic: Intimate Partner Stalking in Aotearoa New Zealand" (2 December 2019) Women's Refuge <www.womensrefuge.org.nz>.

New Zealand Family Violence Clearinghouse "Data Summaries 2015: Snapshot" (2015) <www.nzfvc.org.nz/>

NZCVS "Cycle 2 Key Findings" (2018) <www.justice.com>.

Scoop "Seeking Safety Online" (press release 17 May 2016).

Senate Bill Would Ban Stalking Apps and Save Women's Lives" (4 June 2014) The National Network to End Domestic Violence <www.nnedv.org>.

Stacey Kirk "Strangulation, coercion to marry and family violence to be new crimes with tough sentences – Govt" *Stuff* (online ed, Wellington, 13 September 2016).

Top 5 Apps to Spy On Your Spouse Android Phone" Mobie Spy <www.mobiespy.com>.

UK to criminalise coercive, controlling and psychological abuse" (20 January 2015) New Zealand Family Violence Clearinghouse <www.nzfvc.org.nz>.

Wayne Rumbles (ed) *Electronic Business and Technology Law (NZ)* (online ed, LexisNexis)

Wilhelmina Shrimpton "Calls for better protection for women being stalked by an ex-partner" *Newshub* (online ed, Auckland, 14 October 2019).