The Consumer Spyware Industry

An Australian-based analysis of the threats of consumer spyware

DEAKIN UNIVERSITY

accan

The Consumer Spyware Industry

An Australian-based analysis of the threats of consumer spyware

Dr Adam Molnar and Dr Diarmaid Harkin

August 2019

The Consumer Spyware Industry: An Australian-based analysis of the threats of consumer spyware

Authored by **Dr Adam Molnar and Dr Diarmaid Harkin**

Published in **2019**

The research project was funded by a grant from the Australian Communications Consumer Action Network (ACCAN).

The operation of the Australian Communications Consumer Action Network (ACCAN) is made possible by funding provided by the Commonwealth of Australia under section 593 of the *Telecommunications Act 1997*. This funding is recovered from charges on telecommunications carriers.

Deakin University
Website: https://www.deakin.edu.au/
Email: **adam.molnar@uwaterloo.ca and diarmaid.harkin@deakin.edu.au**
Telephone: **+61 3 925 17645 (Harkin)**

Australian Communications Consumer Action Network (ACCAN)
Website: www.accan.org.au
Email: grants@accan.org.au
Telephone: 02 9288 4000.

If you are deaf, or have a hearing or speech impairment, contact us through the National Relay Service: https://www.communications.gov.au/what-we-do/phone/services-people-disability/accesshub/national-relay-service

ISBN: 978-1-921974-58-8

Cover image: Design by Richard Van Der Male with images from Shutterstock

This work can be cited as: Molnar, A. & Harkin, D. 2019, *The Consumer Spyware Industry: An Australian-based analysis of the threats of consumer spyware*, Australian Communications Consumer Action Network, Sydney.

Table of Contents

Figures and Tables

Acknowledgements

We would like to acknowledge the terrific research assistance support of Ms Erica Vowles and Mr Tom Andrews. Likewise, the staff at *HackLabs,* particularly Petr Novak, who undertook elements of the technical analysis. We would also like to thank researchers at Citizen Lab for building out important aspects of the analysis initiated in this project, including Christopher Parsons, Jakub Dalek, Cynthia Khoo, Miles Kenyon, and Jeffrey Knockel. Karen Bentley and Kaofeng Lee from the Women's Services Network (WESNET) also helped develop our understanding of the threat of spyware in the context of family violence. We are very grateful for your support.

Finally, we would also like to acknowledge the support of Tanya Karliychuk and the team at ACCAN. They have been a tremendous help throughout this project. Any errors or omissions in the information contained in this report are the responsibility of the authors.

Executive Summary

- Invasive surveillance software known as “spyware” is available for general consumption within Australia. There are multiple products available that allow everyday consumers the ability to place a smartphone under close surveillance. This can include capturing SMS message data from the phone, voice-recordings of phone conversations, internet browsing data, private videos or photos, in addition to some spyware allowing ‘live’ access to the phone’s camera and/or microphone. Certain spyware products also contain other features such as the ability to send ‘spoofed’ SMS messages that assume the identity of a captured device. All of the above can be performed in ‘stealth’ without the knowledge of the targeted device’s owner.
- We conducted several types of analysis to uncover the threat of the consumer spyware industry for Australia. We performed a market analysis to help identify the most popular spyware products used in Australia. After identifying a sample of 9 spyware products, we subjected these companies to in-depth scrutiny that included examining their marketing material, their terms of service, privacy policies and other corporate documents. Furthermore, we undertook a user analysis of the spyware, installing it on smartphones and testing how they operate within the Android and iOS environment. We also subjected this sample to technical analysis with the support of cyber security consultants ‘HackLabs’. Finally, we also examined the legal context in Australia in relation to the possession, production, distribution, and use of spyware.
- Our research findings suggest that spyware is a particularly acute threat in the context of domestic and family violence, with multiple spyware companies encouraging and promoting the use of spyware against intimate partners. Children are also commonly suggested as a target for spyware.
- In principle, the selling, possession and/or usage of spyware violates a variety of Australian laws. Moreover, while spyware companies are covered under the *Privacy Act 1988*, many of their activities violate the Australian Privacy Principles (APPs). In practice, prosecuting producers or abusive users of spyware faces a number of challenges that undermine the regulatory capacity of the law. This undermines the overall possibilities of a law enforcement approach to tackling spyware companies, but law enforcement agencies and regulatory agencies could use existing laws to minimise the abusive use of spyware within Australia with a greater understanding of the threat.
- When comparing Android phones with iPhones, the Android operating system is significantly more permissive of spyware accessing critical phone functions and confidential data. This means that Android users carry a higher risk of being subject to spyware than iPhone users. But it should be noted that iPhone users are not immune and still need to take reasonable precautions.
- Technical analysis of spyware reveals that software developed within the consumer spyware

industry often exhibits extremely poor data security practices. For instance, inadequate precautions are taken to protect or encrypt data whilst it is in transit. This creates additional risks for the exposure of highly sensitive personal information and data.

- Technical analysis also reveals that spyware products rely extensively on third-party companies to deliver their services. For instance, they may use intermediaries to host data. While it may be difficult to constrict the development of spyware by targeting the spyware companies themselves, third-party intermediaries such as Codero, Cloudflare Inc, Rackspace IT, and NForce Entertainment B.V. could be convinced to withdraw technical support for notorious spyware vendors.
- While offensive strategies for disrupting spyware companies operating online (and across multiple legal jurisdictions) are difficult, Australian authorities and organisations can help promote 'defensive strategies'. This can include leveraging influence over intermediaries or commercial actors who may inadvertently host or facilitate spyware (such as Google permitting the sale of Cerberus on its Play Store). The Office of the Australian Information Commissioner (OAIC) also has recourse against poor practices of spyware companies, which could spur changes in how spyware companies' products presently operate to the detriment of the security and safety of consumers, particularly women and children. Likewise, awareness and information campaigns can be utilised to promote greater understanding of the threat, and how to counter it. See for example, materials that we produced for the Women's Services Network (WESNET 2019).
- We argue that proposed amendments to the Privacy Act 1988 (Commonwealth), set for the latter half of 2019, should explicitly consider amendments that would further protect the personal information of individuals from the use of consumer spyware--most notably for the protection of women and children.
- In spite of our research on the technical, legal, and policy aspects toward more effective regulation of spyware companies as detailed in this report, we wish to remind readers that the specific issue of technology-facilitated abuse and harassment through the use of spyware is inseparable from our broader culture of patriarchal and gendered discrimination that disproportionately impacts women, children, and non-binary persons. While the insights generated in this report may provide useful avenues for reining in a largely unregulated and industry, we insist that any steps to transcend forms of technology-facilitated abuse must also critically address broader social and ethical values.

Introduction

Invasive surveillance software, known as 'spyware', is presently available to general consumer audiences. A sizeable market has emerged of a number of companies who sell spyware targeted at consumers who wish to place a smartphone or personal computer under intensive monitoring. This research focused exclusively on smartphones and discovered that it is relatively easy to purchase software that can remotely collect text messages, phone conversation recordings, GPS location data, and access the camera of a targeted device. Crucially, this data can be collected 'by stealth' with the user of the device having no indicators that their privacy is being compromised.

The widespread availability of spyware therefore, creates clear risks that this software can be used abusively. It is easy to anticipate that spyware will be used to violate individual's privacy and that compromised data will be used as an aid for harassment, intimidation, bullying, and coercion. Abusive use of spyware has already been widely documented in the context of domestic and family violence. Women's Aid (2018) in the UK report that 29% of abuse victims experienced the "use of spyware or GPS locators", in 2017 there were 130 reported cases of spyware to the UK's National Stalking Helpline (Lyons 2018), and in the US, there have been a number of notable homicide cases wherein perpetrators tracked their victims through the use of spyware (Citron 2015).

Beyond domestic and family violence, spyware is also a threat to general privacy. Deploying spyware against an individual without their knowledge is a clear violation of their human right to privacy (Article 12, UDHR), and as will be explored in later chapters of this report, in violation of multiple laws within Australia. It is neither morally or legally acceptable to 'spy' on others and yet multiple 'spyware' vendors eagerly advertise the 'spying' capabilities of their product. Consider, for example, the names of spyware companies: 'MSpy', 'FlexiSpy', 'TheTruthSpy', and 'SpyEra'.

Consumer spyware is a threat to digital privacy. It could act to undermine digital confidence in the privacy of our smartphones, and it should always be emphasized that it is a particularly acute danger to victims of domestic and family violence. Combatting the abusive threat of consumer spyware is therefore urgently required. It is necessary to explore the policy options of limiting, mitigating, and if possible, eliminating, the threat of spyware. This report will hopefully offer a contribution to this goal.

What is 'spyware'?

'Spyware' is a label given to software that is developed for the purposes of spying or used in the context of spying. It is important to note that the software itself is just computer code, and therefore, in a sense, morally 'neutral'. Code becomes spyware when it is applied in a specific social context and given that label by a community. There are areas of confusion, for instance, around how spyware may differentiate from legitimate programs that share confidential data from smartphones. Therefore, there are semantic issues around the definition of spyware that need to be clarified.

For the purposes of this report, we consider a program to be 'spyware' if the following key features

are present (see also Harkin et al 2019: 4-5):

1. Data is gathered remotely from a target device that would not otherwise be shared unless foreign code or software was introduced or permitted access by an operator.

2. Data is gathered from the target device with the credible possibility that the user of the target device would not be aware of the exfiltrated information, the on-going presence of the foreign code or software, or any permission to disclose information.

3. The code or software is to be deployed in the context of targeting a specific individual or group of individuals for the purposes of monitoring, tracking and surveillance. It therefore does not include firmware updates, native operating system functions, or applications that collect large amounts of data from multiple users in the user-approved course of its 'normal' functioning (e.g. Facebook or other social networking services and platforms).

4. The data being disclosed to operators about the target can be reasonably understood to include private, confidential and otherwise intimate personal information (such as location data, private correspondence, personal photos, passwords etc.)

What are the capabilities of spyware?

Not all spyware is alike, and programs differ in their capabilities. The type of data that spyware is able to capture depends upon the programming of the spyware, the method of how the data is compromised, the technical skill of the installing party, and also the operating system environment in which the spyware is placed. On this latter point, for instance, the Android operating system is significantly permissive of spyware accessing the phone's GPS features or camera. This compares unfavourably with the iOS operating system where there are no current spyware options for gaining access to the camera of an iPhone surreptitiously (without jail-breaking the device, i.e. installing third-party software that overrides the native security features of the device). Comparatively, with Android phones, programs are available on the Google Play Store that can provide real-time photo or video extracted from the device without the target's reasonable knowledge.

While it is much 'simpler' to find programs in the Android environment to gain access to a target's camera, private messages, GPS location, and other confidential data sources, spyware with significantly invasive capabilities can be purchased for both Android and iOS phones. It is worth outlining, therefore, the 'worst case scenario' to identify the full range of capabilities of consumer spyware. In this research we were capable of jail-breaking an iPhone X and installing 'Flexispy'. We confirmed that the spyware was able to compromise a range of critical features on the device. In the 'lab environment', the spyware was placed on the iPhone X and the research team simulated normal phone use by making calls, travelling through the city, browsing on the internet, checking emails, using social media platforms, taking pictures, and sending confidential SMS messages. While a 'target' used the phone, an 'operator' research assistant would sit at a remote location and access private data from the phone via an internet portal provided by the spyware vendor.

From this experiment, we confirmed that spyware of this type could capture the following data without the user of the phone having any idea that the phone was leaking this information:

- GPS location
- Recordings of any phone-calls made by the device
- Recording of any VoIP calls made by the device (including Skype and Facetime)
- SMS messages
- Data within other messaging systems such as Facebook Messenger and WhatsApp
- Emails
- Photos and videos
- Notes
- Calendar information
- Internet browsing activity
- Call logs
- The names and numbers of contacts in the 'address book'

There were also a number of other functions of 'Flexispy' that were considerably alarming:

- The operator could remotely command the spyware to send live pictures and video from the cameras on the target device without the user being aware the cameras were active.
- The operator could 'call-in' to the phone from a pre-assigned number and listen to the ambient audio, thus turning the phone into an audio 'bug' (the user would have no indication that this is happening).
- The operator could request periodic screen-grabs from the target-device, thus getting a sense of what the user was looking at on their phone.
- Flexispy provides 'keylogger' information. Thus, it tells the operator everything that was typed by the user on their keypad. This is a method for uncovering passwords to private accounts owned by the user.
- Flexispy would also allow the operator to send 'spoof' SMS messages from the device. Messages could be sent to contacts of the user and it would appear to come from the user, but the message was actually authored by the operator. Thus, there is an ability to impersonate the phone user without their knowledge.

The above capabilities of Flexispy represent a 'worst-case' scenario when your device has been compromised by spyware. There are many spyware vendors that offer software that has the same or similar abilities as Flexispy on both Android and iOS devices. There are other spyware options that offer only some of the capabilities outlined above. For instance, 'TeenSafe' provided live GPS tracking, but did not access the cameras of the target device. Whether or not particular spyware compromises a large amount of phone functions or a small set of functions depends upon the

factors outlined earlier. It should be noted however, that even a relatively small set of functions being compromised, such as GPS location and SMS messages, could have significant ramifications for victims of family violence, for example.

What is 'consumer' spyware?

This report makes repeated reference to 'consumer' spyware. This is a deliberate choice to differentiate between spyware that is sold to general audiences ('consumer' spyware), and spyware that is deployed in contexts of law enforcement, state espionage, and corporate espionage. It should be noted that there is a difference between 'high-end' spyware that is sold to very wealthy, powerful actors such as nation-states, and the spyware considered here. There is a clandestine, elite market for spyware amongst a pool of customers that are seeking an ability to engage in remote access to targeted devices. As an example, the Israeli technology firm NSO Group has been known to develop exploits of iOS that has been used by governments such as the UAE (Marczak and Scott-Railton 2016). In one circumstance, it was reported that NSO Group sold an iOS 6 exploit kit for $18 million dollars (Brewster 2016).

While concerning in their own right, markets for such boutique spyware should be considered as a relatively distinct phenomenon when compared with consumer spyware. Firstly, they are far more costly and can only be purchased by a limited set of customers, often nation-states. Secondly, they are much more likely to be targeted at specific individuals or groups such as journalists, activists, political figures, and individuals under investigation from law enforcement bodies. And thirdly, the market for such spyware is deliberately clandestine and hidden from ordinary consumers in order to preserve the viability of the exploits they rely upon. If knowledge of the exploit was made available on an open market, the developers of iOS or Android systems could issue security updates, thus rendering the exploit redundant. Hence, the market is relatively closed, and only available to 'high-end' customers who are willing to pay a premium for a product that affords remote access to digital devices.

In comparison, the 'consumer spyware industry' refers to the collection of companies and vendors who target their product at anyone willing to purchase through a relatively affordable 'subscription-based' business model. These are the companies whose products are visible from a search engine result and show no discrimination in who they sell their software to. Given the broad accessibility of this type of spyware to a general consumer audience, it is this 'consumer spyware industry' that is most relevant to issues such as family and domestic violence. It is also the exclusive focus of the research presented here.

What did this research do? An overview of the investigation

Our investigation into the consumer spyware industry had a number of different elements. The core research team recruited a number of research assistants to aid with the investigation and also utilised the expertise of a security consulting company, 'HackLabs'. The overall goal of the research was to capture as much information about the threat of consumer spyware as possible, and to develop strategies for suitable policy responses.

To achieve this aim, we undertook a number of different tasks:

- Market analysis

The research team conducted an overview analysis of the consumer spyware market. We undertook steps to gauge the range of products offered by spyware vendors, the type of spyware-attacks being sold, and identified the most prominent vendors on the market. This analysis concluded with us identifying 9 spyware vendors for closer scrutiny, including a follow-on technical analysis of a more narrow subset of these companies.

- Content analysis of the websites and marketing materials of spyware vendors

A sample of 9 spyware products was identified to examine how these products were marketed. The content of their websites was systematically scrutinised to establish how they presented their product and how the vendor suggested the product should be deployed. This analysis identified which groups were suggested as targets of spyware and what the supposed 'legitimate' use of this product was according to the vendor.

- Corporate policy analysis

The sample of 9 spyware products was also subject to an analysis of their privacy policy and terms of service. Their privacy policies were systematically scrutinised to identify whether they had adequate procedures and policies in place to account for the obvious risks of abusive data use. We subsequently evaluated these privacy policies in relation to Australia's *Privacy Act* 1988.

- User analysis

9 different spyware products were purchased and deployed onto Android and iOS phones. The goal of user-analysis was to determine how the spyware 'works' from the perspective of the installing-party (the 'operator'), and also the user of the compromised phone (the 'target'). When the spyware was installed on each device we purposefully generated data on the phone to observe what data was leaked, and under what conditions. It should be noted that some companies only sold products for use on iOS, and some only for Android. Some companies sold to both. When companies sold to both operating systems (OS), we would install a version on each OS to observe any notable differences in functionality.

- Technical analysis by HackLabs

9 spyware products were also targeted for digital forensic analysis by the expert security consultancy firm, HackLabs. The goal of the forensic analysis was to examine how the spyware operated at a programmatic and network-traffic level. The aim was to understand and critically evaluate the mechanisms through which the spyware operated and shared confidential information with the spyware companies' servers.

- Legal analysis

Finally, a cursory legal analysis was also performed to understand the range of potential laws that spyware might violate within Australia. This was from the perspective of selling spyware, purchasing spyware, and deploying spyware against an unwitting target. The analysis considered the differing jurisdictions across Australia including states, territories, and Commonwealth legislation. The information contained in this analysis should not be considered as legal advice.

What do we know about the spyware industry?

This section will briefly detail what we know about the spyware industry from previous research by journalists and academics. Information about the spyware industry has been hard to obtain given that it is an inherently secretive world. This is particularly true of the market for 'high-end' spyware and elite purchasers. Research centers such as 'The Citizen Lab' (McKune and Deibert 2017), advocacy groups such as Privacy International (Privacy International 2018), and investigative reporters (see for example Cox 2017; Valentino-DeVries 2018) have done terrific work uncovering the limited information we have. Another key avenue of discovery has been in circumstances where hackers have targeted spyware vendors to reveal embarrassing information. Hackers, for instance, targeted the Italian-based spyware firm 'Hacking Team' and published internal confidential, company documents (Hern 2015).

Likewise, there is also a trend of consumer spyware companies having unsecured servers that has exposed client information and confidential data about the company. As examples, a security researcher discovered that TeenSafe servers left customers email addresses and their passwords exposed (Whittaker 2018), and Vice Motherboard recently reported that Mobiispy had left 95,000 images and 25,000 audio recordings on an unsecured server that was accessible to anyone (Franceschi-Bicchierai 2019a; Franceschi-Bicchierai 2019b). Often the incompetence of spyware vendors can inadvertently reveal key information and reports outline that 12 different spyware companies have had serious breaches in the past two years (Franceschi-Bicchierai 2019a).

In terms of the users of spyware, it is has been thoroughly demonstrated that governments have been purchasing spyware from vendors for years. Citizen Lab, in particular, have exposed and revealed abusive use by the Ethiopian government (Marczak et al 2015a), the government of the UAE (Marczak and Scott-Railton 2016), and strongly suspect 33 different governments of using 'FinFisher' software developed by the English-German firm 'Gamma International' (Marczak et al 2015b). It has therefore been suggested that the 'high-end' spyware industry has been "at least partly subsidized by the public sector" with certain development teams receiving "de facto state support" (Buckart and McCourt 2017: 40-41). The British Government, for instance, has licensed the sale of spyware to the governments of Honduras, Saudi Arabia, Bahrain, Turkey and Egypt, despite the recognised and credible expectation that such software could and would be used for human rights abuses (Lakhani 2018).

On the general consumer side, reliable information on the number of customers of spyware has been largely elusive, but hacks have revealed that 'Retina-X' and 'Flexispy' have at least 130,000 general-use customers (Franceschi-Bicchierai and Cox 2017). Spyware companies tend to exaggerate the amount of customers they have with TeenSafe claiming to have over a million clients, but leaked customer data may suggest that number is closer to 10,000 subscribers (Whittaker 2018). Likewise, on some reports, 'mSpy' is said to have 2 million users (Cottle 2014), but have elsewhere stated that around 27,000 Americans subscribed to their service in the first quarter of 2018 (Valentino-DeVries 2018). Exact figures on the number of users of spyware will continue to remain unclear.

There has been one notable case of a spyware vendor facing legal proceedings, and that was the creator of 'StealthGenie' being prosecuted by the U.S Department of Justice (DOJ 2014). He was fined $500,000 USD and the FBI was capable of disabling the website hosting 'StealthGenie' (ibid). This conviction was made possible because the developer and the host service were geographically present in the United States, and the FBI took a sufficient interest to investigate (Timberg and Zaptotosky 2014). Otherwise, concrete knowledge of the spyware industry has been limited to select media exposés and data leaks. In 2013, a UN *Special Rapporteur* suggested that the industry "is virtually unregulated as States have failed to keep pace with technological and political developments" (La Rue 2013: 75). Academic observers have also noted that "the commodity chain for hacking products and services has evaded comprehensive, or even substantial, regulation to date" (Burkart and McCourt 2017: 49). As a result, information on the industry can be difficult to establish and it will be extremely difficult to gain an exhaustive understanding of the range of spyware vendors in the market and the scale of use 'in the field'.

Consumer Spyware Marketing Materials: A Content Analysis

General consumers can easily find many websites dedicated to selling consumer spyware. There are a wide range of companies selling broadly similar software and their products can be found through a simple search-engine inquiry. This research narrowed in on 9 spyware products that we believed were the most prominent in the context of Australia. Using 'Google Trends' data we were able to make an approximate determination of which spyware is featured most often in Google searches within Australia. As a result, we selected a sample of 9 spyware products that we chose for closer content and technical analysis.

Our content analysis focused on 9 different spyware vendors.

1. mSpy
2. Hoverwatch
3. Flexispy
4. TheTruthSpy
5. Highster Mobile
6. Teensafe
7. Mobistealth
8. Cerberus
9. Trackview

This section outlines the results of our content analysis of the above spyware vendors. The goal of the content analysis was to examine how the spyware marketed itself. We were interested in determining how spyware vendors attempted to present a 'legitimate' use of its product, and what were the social contexts in which they suggested this software should be used? As we have outlined in an academic paper (see Harkin, Molnar and Vowles 2019), spyware companies have a fraught marketing challenge: their product can only be deployed in limited contexts without violating privacy laws, and it has a close reputational association with forms of intimate partner abuse. Furthermore, the notion of 'spying' on someone is morally and socially unacceptable. Therefore, it is interesting to observe how spyware vendors attempt to justify and present their product.

We systematically examined the websites of each of these spyware vendors. It should be noted that two of the spyware products can be found in the Google Play Store (Cerberus and Trackview), while one can be found in the Apple App Store (Trackview). We also examined how these products presented themselves within those app stores. Here are the chief observations from an analysis of the marketing materials of various spyware vendors:

Children, employees, intimate partners, and thieves are depicted as the principal targets of spyware

Across our sample, there was a clear theme that the main targets of spyware were children, employees, intimate partners, and thieves. See the table below for an overview of how each vendor chooses to frame their product (see also Harkin et al 2019: 12).

Table 1 Showing an overview of the different suggested contexts in which spyware should be used according to our sample vendors

Spyware vendor:	Explicit suggestion to use the software targeting children?	Explicit suggestion to use the software targeting employees?	Explicit suggestion to use the software targeting intimate partners?	Explicit suggestion to use the software for anti-theft purposes?
MSpy	Yes	Yes	No	Yes
Hoverwatch	Yes	Yes	Yes	No
Flexispy	Yes	Yes	No. However, on their video tutorial there is a reference under "Why do you need Flexispy?" to "Protect your relationships. Lasting relationships are built on trust. Make sure yours is too." It should be noted that Flexispy has been more explicit with this purpose in the past (see Cox 2017).	No
TheTruthSpy	Yes	Yes	Yes	Yes

Spyware vendor:	Explicit suggestion to use the software targeting children?	Explicit suggestion to use the software targeting employees?	Explicit suggestion to use the software targeting intimate partners?	Explicit suggestion to use the software for anti-theft purposes?
Highster Mobile	Yes	Yes	One reference is made to monitoring "those in relationships" on their website description depicted on the google search-results page.	Yes
TeenSafe	Yes	No	No	No
Mobistealth	Yes	Yes	No	No
Cerberus	No	No	No	Yes
Trackview	Yes	Yes	Yes	Yes

As can be seen from **Table 1** there are variations in how individual spyware vendors suggest their product should be used. The majority of vendors made reference to either monitoring children or monitoring employees, while a smaller sample choose to suggest using spyware for monitoring an intimate partner. **Figure 1** shows the chief marketing message from the website of MSpy that places a primary emphasis on monitoring children for the "ultimate…parental control" (see also Harkin et al 2019: 13).

Figure 1: the chief marketing message on the MSpy website.

Considering the associations of spyware with intimate partner abuse, it is not surprising that many vendors choose not to suggest using spyware in this context. However, several of the vendors on our sample explicitly recommended using spyware to monitor intimate partners. Most notably, TheTruthSpy suggests deploying spyware on “your lovers” (see **Figure 2**), while Hoverwatch provides a blogpost outlining how to “track potentially cheating spouses (see **Figure 3**) (see also Harkin et al 2019: 13).

Figure 2: suggested uses of TheTruthSpy.

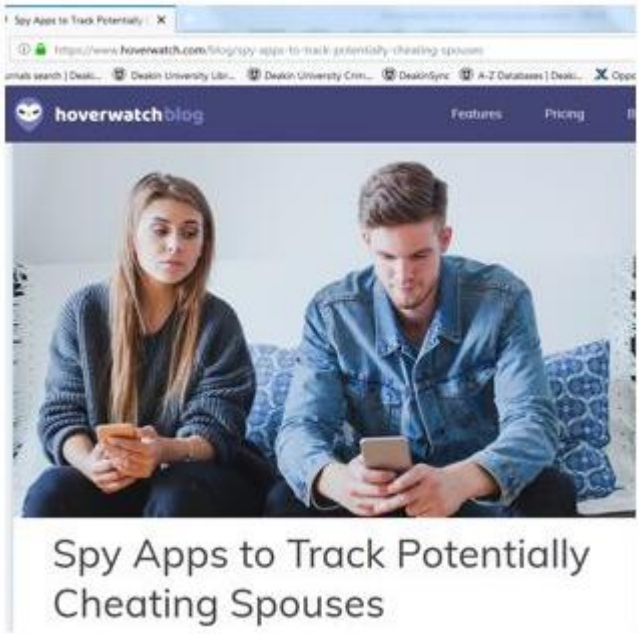

Figure 3: blogpost on the website of Hoverwatch

Furthermore, Trackview suggests real-time GPS tracking of “your spouse”, and two other spyware vendors have limited references to monitoring intimate partners. Flexispy has a tutorial video that suggests you can “protect your relationships” and the website description for Highster states that it can be used to monitor “those in relationships”. Flexispy has been more prominent in the past about

encouraging use against intimate partners (see Cox 2017), but has since attempted to remove all references to intimate-partner tracking.

The level of surveillance power of the spyware goes beyond proportionate 'monitoring'

While the various spyware vendors attempt to suggest their products should be used in the context of 'monitoring' employees or family members, the surveillance power of their products often outstrip what could be understood as proportionate or ethical 'monitoring'. It may be conceivable that parents or employers may have a legitimate contextual reason for needing to locate children or employees via GPS (as an example), however, the range of functions offered by most of the spyware we examined exceeds what could be understood as proportionate or ethical 'monitoring'.

As an example, **Figure 4** below outlines the range of data that is shared from a device once Flexispy has been installed (see also Harkin et al 2019: 13).

- ✓ Phone Call recording
- ✓ Phone Call interception
- ✓ FaceTime Call Recording
- ✓ Spycall
- ✓ Environment recording
- ✓ Facebook Call Recording
- ✓ LINE Call Recording
- ✓ Skype Call Recording
- ✓ Viber Call Recording
- ✓ Whatsapp Call Recording
- ✓ SMS Keyword deletion
- ✓ RemCam
- ✓ RemVid
- ✓ Spoof SMS
- ✓ Call logs
- ✓ FaceTime Call logs
- ✓ Facebook Call Logs
- ✓ LINE Call Logs
- ✓ Skype Call Logs
- ✓ Viber Call Logs
- ✓ WeChat Call logs
- ✓ Address book

- ✓ SMS messages
- ✓ MMS
- ✓ iMessage
- ✓ Facebook Messenger
- ✓ Instagram Direct Messages
- ✓ LINE Messages
- ✓ Skype Messages
- ✓ Viber Messages
- ✓ Whatsapp Messages
- ✓ BBM Messages
- ✓ Hangout Messages
- ✓ Tinder Messages
- ✓ WeChat Message
- ✓ Browsing activity
- ✓ Browser bookmarks
- ✓ Email
- ✓ Application activity
- ✓ Installed applications
- ✓ Application Screenshots
- ✓ Keylogger
- ✓ Photos
- ✓ Videos

- ✓ Audio files
- ✓ Wallpaper images
- ✓ Notes
- ✓ Calendar
- ✓ Location tracking
- ✓ Visibility Option
- ✓ SIM Changed Notification
- ✓ Automatic Remote Updates
- ✓ Free Updates

Figure 4: the full suite of data that is provided to Flexispy when the spyware is installed on the device

As can be seen above, Flexispy shares an enormous scope of data and destroys any sense of privacy for the user of the phone. It captures recordings of phone-calls, SMS messages, messages sent via third-party applications like WhatsAPP, emails, and VoIP calls, and reveals any pictures or videos taken by the phone. It also captures keylogger information, and allows the operator to access the camera or microphone of the device without any notification to the user.

It should be noted at this point that spyware's expansive data collection capabilities are sufficiently wide as to not only compromise the private data of the user of the device, but anyone who also interacts with the user via their device. For instance, if a third party sends messages or engages in a phone conversation with the user of the device, their privacy will also be compromised. Therefore, if hypothetically, a parent deployed this program with their child, they would then be obligated to inform their child's friends (and the friends' parents) that this program was in place, lest they obtain private information without consent. A school, for instance, would need to be informed that a child had a device that the parents could 'eavesdrop' in at will (which would be unlikely to be permitted). The consent of third-party information has not been considered or countenanced in any of the spyware vendor's marketing materials or legal and privacy policies.

In this regard, it is hard to reconcile the notion that spyware of this kind could serve a legitimate, ethical 'monitoring' function, when compared to the sweeping scale of data that is scooped up in the programs' dragnet. Furthermore, as can also be observed from some of the functions above, the capabilities of the spyware also go beyond a 'monitoring' posture. Flexispy (and other spyware vendors) offer 'spoof SMS' functionality, for example. Spoofing an SMS from a device is more akin to an impersonation feature. It involves 'faking' authorship of a message to make it appear that a message came from the user of the device when it would have been authored by the unseen operator. While the spyware vendors maintain that these products are to be deployed for the purposes of 'monitoring', this marketing message is often betrayed by the provision of impersonation functionalities, thus undermining the possibility for ethical and legitimate use of these products.

There are clashes between legal disclaimers that emphasise consensual use and marketing claims that suggest secretive use

There is also conflict between the marketing of spyware products that often emphasise and highlight the possibility of using the product secretively, and legal disclaimers that often feature in the 'small-print' sections of spyware websites. Spyware vendors are aware that their products could be used abusively and therefore typically include a disclaimer or notification warning the purchaser that they are to obtain the consent of the target before deploying the software. For example, see **Figure 5** for the disclaimer featuring on the website for Highster Mobile outlining that installing Highster Mobile on someone's device without their knowledge is likely to be "illegal":

Installing Highster Mobile, you represent that Highster Mobile will be used in only a lawful manner. Logging other people's Cell Phone or Computer data or installing Highster Mobile on another person's Phone/Computer without their knowledge can be considered as an illegal activity in your country. Highster Mobile assumes no liability and is not responsible for any misuse or damage. It is the final user's responsibility to obey all laws in their country and/or state.

Figure 5: a portion of the legal disclaimer from the website of HIghster Mobile

Yet, elsewhere on the website of Highster Mobile, it encourages and promises secretive and non-consensual deployment of the software. See **Figure 6**.

The most important thing about the Highster Mobile, a contact free spy cell phone download, is that it can monitor the other cell phone remotely. This means that you do not need to have the target cell phone in your hands for you to install it. The Highster Mobile can be installed even without having the cell phone of the targeted person at hand. This will ensure that your confidentiality is catered for and that the other person does not get to know that you are spying on them because no evidence will be left for them to know that you are spying on them. Your privacy and confidentiality is therefore guaranteed. All you need to do to spy on the other person using the Highster Mobile spy software is just to input the number of the other person and the process of installation is completed. Your child will never know that you are spying on them and no form of guilt and worry will come your way because the process is legal and promises your confidentiality.

Figure 6: claims made by Highster Mobile in their marketing materials outlining how it can be deployed secretively against a non-consenting target. (Note that in this marketing material, Highster Mobile also promises remote installation of spyware. This is a misleading claim. Highster Mobile cannot be installed remotely).

A number of spyware vendors follow a similar pattern of emphasising the ability to 'spy' secretively without the target's knowledge in their marketing materials, but then suggest in the legal disclaimers that the product should only be deployed with the consent of the target. Both of these things cannot be true at once, therefore there is a conflict in how spyware vendors present their product.

There are no clear options for abused parties to address the spyware vendor

Finally, despite the recognised scope for abuse of spyware, there are no clear options or guidance for abused parties to engage with the spyware vendors regarding their compromised data. In all of our content analysis that engaged with marketing materials, website materials, and terms of use in addition to legal and privacy policies of spyware, there was no explicit mention of how victims of spyware could possibly engage with the spyware vendor to report or recover data extracted in a non-consensual context. No support mechanisms are offered for victims of abusive use. It should be noted that vendors generally provided an email address or online form in the event of a complaint

or request for technical support by the operator, but provided no specific guidance for how violated parties could enquire about the fate of their private data. In this regard, the 'voice' of the marketing and privacy materials of spyware products speaks to the concerns of the purchaser/operator and does not address potentially abused parties. This is a major oversight on the part of the spyware companies, particularly in light of the significant scope for abuse using these products. It should be an ethical imperative for these companies to support abused individuals who are aiming to obtain information about the fate of their confidential data.

Consumer Spyware in Australia: A Legal Review

This section reports on the variety of legislation currently in place within Australia that is relevant to the regulation and use of consumer spyware. It offers an overview of the legal mechanisms presently available to address abusive use of spyware, and a brief guide for issues regarding the legal regulation of this form of surveillance. It takes account of the various legal jurisdictions within Australia including the statutory variations between the states, territories, and the Commonwealth.

Before detailing specific legislation, it is important to outline some points regarding the legal complexities of regulating spyware. Firstly, 'spyware' products provide different functionality and share different types of data. Therefore, different spyware products may violate different laws. For instance, some of the spyware products reviewed by this research offered 'spoof' SMS functions, which uniquely violate Fraud and/or Identity Theft legislation because of its impersonation aspect. Likewise, depending on the gravity of the type data shared (consider technical device information versus live-access to the camera), this has ramifications for which legislation is relevant to particular circumstances. In other words, it will be context specific as to which laws are relevant in any instance of abuse, depending on the functionalities of the spyware being used and the type of data shared by the software. There are no uniform set of laws that a generic understanding of 'spyware' violates.

Secondly, the use of spyware creates data jurisdiction and offence jurisdiction issues. It is often possible (and likely) that the vendor of spyware, the user of the spyware, and the target of the spyware are operating in different jurisdictions. Likewise, the data in question is often transmitted by spyware across jurisdictions and stored on servers in countries other than Australia. These jurisdictional complexities create issues for the relevancy of certain laws, the ability to collect evidence, and the ability to prosecute or regulate certain parties.

Third, there are multiple parties who have differing legal standing when spyware is used. This includes the target who is subject to the spyware on their personal device; the 'operator', who is the party that purchased the spyware and now has operational control over some of its uses and access to the exfiltrated data; the vendor of the spyware who has created the software and provides the infrastructure for the operator to access the exfiltrated data and may also host the data; intermediaries such as cloud hosting companies that facilitate the carriage of the spyware companies' products and services; and third-parties who interact with the target and the target's device, and who therefore will also have their data scooped up by the spyware's dragnet (consider for example, sending an SMS to the target's phone, providing an intimate picture, or being present while camera footage or audio is captured by the compromised device). In any given circumstance, these various parties have differing or unique legal responsibilities, legal standings and legal interests.

Finally, the context in which the spyware is used can introduce additional relevant legislation. As illustrated earlier, spyware is often used to target children, employees or intimate partners. For each of these groups, there are unique legal implications to be considered. For instance, Australian statutory bodies are signatories to the *United Nations Convention on the Rights of the Child,* where

article 16 states that children ought not to be "subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence" (OHCHR 2019). This would be uniquely relevant in the circumstance that a child was targeted with spyware. Workplace legislation would be relevant in the circumstances of spyware deployed against employees, and when intimate partners are targeted, family violence legislation is relevant. For example, the *Family Law Act 1975* (Commonwealth) includes coercion or control within the definition of family violence, along with "stalking" that could be pertinent to instances of spyware use. Likewise, the Magistrates Court of Victoria issues *Family Violence Intervention Orders* that prohibit the respondent from "attempting to locate or follow the protected person or keeping them under surveillance" (Victoria Legal Aid 2019). Therefore, depending on the target of the spyware or the context within which it was deployed, additional legislation or frameworks ought to be considered.

Considering these multiple complexities, an exhaustive guide to all the legislation or statutory instruments that are relevant in circumstances where spyware is used abusively cannot be established within the scope of this report. Instead, we offer a useful overview of the legal landscape, highlighting the most relevant legislation. What follows is intended as a guide for subsequent detailed legal analysis, and should not be considered as legal advice in itself. Thanks to Mr Tom Andrews for his help with this analysis.

Is it legal to create, sell, or possess spyware in Australia?

In principle, the creation, selling and possession of spyware in Australia could potentially violate the *Telecommunications Offences and Other Measures Act 2004* (Commonwealth) that outlines that it is an offence if a person "manufactures", "advertises, displays or offers for sale", "sells", or "possesses" an "interception device" (474.4). In this context, a "interception device" is a device that "is capable of being used to enable a person to intercept a communication passing over a telecommunications system" and "could reasonably be regarded as having been designed" for the purposes of being used "in connection with the interception of communications passing over a telecommunications system". (Exceptions are available to law enforcement and forms of engineering maintenance carried out by telecommunications services.)

In practice, however, the above legislation has not been tested with the example of spyware. In such circumstances, a court would need to accept that spyware constitutes "an apparatus or device"; that the purpose of the software can be objectively interpreted as being used "in connection with the interception of communications passing over a telecommunications system"; and that capturing of data from a smart-phone by spyware constitutes an "interception" (rather than a theft of data or unauthorized access to data, for example).

Until this is tested within court proceedings this is a theoretical position, but if a court agreed to the above interpretations, it would be a criminal offence to produce, advertise, or possess spyware. To date however, no Australian case law exists to test any of these assumptions. Furthermore, the practical and jurisdictional difficulties of targeting spyware vendors or identifying individuals in possession of spyware, and the unlikelihood of this issue being pursued by any enforcement body makes it is unlikely that test cases or prosecutions will be forthcoming.

What potential laws are breached when spyware is deployed abusively?

Unless spyware is deployed with clear two-party consent between the operator and the target, the operator is likely to violate a range of Australian laws. This could include laws relating to harassment, stalking, fraud, identity theft, surveillance devices, computer offences, telecommunication offences, and breach of confidence. Across Australia variations exist in how each of these offences are understood, with differing Acts for the States and Territories often containing their own unique provisions or wording. To that end, this report will not exhaustively outline each jurisdictional variation and its subsequent ramifications for prosecuting abusive use of spyware, but will provide a guide to the types of legislation that could hypothetically be applied.

Surveillance Devices Legislation

Across Australia, the various jurisdictions often have specific legislation relating to surveillance devices. Most of this legislation concerns itself with the use of devices by law enforcement, but often has ramifications for non-state users of surveillance technology. As an example, in Victoria, the *Surveillance Devices Act 1999* (Vic) contains provisions relating to the use of 'listening devices', 'optical surveillance devices', 'tracking devices', and also a 'prohibition on communication or publication of private conversations or activities' that could all be relevant to the abusive use of spyware.

Telecommunications Offences

As outlined earlier, the *Telecommunications Offences and Other Measures Act 2004* (Commonwealth) potentially makes it an offence to possess spyware, but the Act also contains a number of other provisions that are relevant here. For instance, "using a carriage service to menace, harass or cause offence" (474.17), or the "wrongful delivery of communications" (474.5). It is possible to anticipate that a court would rule that using spyware in the context of intimate partner abuse constitutes "menacing" conduct (474.17), and that an abuser using spyware to snoop on emails or text messages is therefore causing a "communication to be received by a person or carriage service other than the person or service to whom it is directed" (474.5). Furthermore, if spyware was used as an aide to other offending, such as a homicide, it is conceivable that "Using a telecommunications network with intention to commit a serious offence" (474.14) would add an additional charge to the principal offence.

Computer Offences

In circumstances where courts are willing to consider that a smartphone is a "computer", the states, territories and Commonwealth have varieties of computer offences that would be relevant. Notably, for instance, the Commonwealth's *Criminal Code Act 1995* makes it an offence if a person causes "unauthorised access to data held in a computer", "unauthorised modification of data held in a computer" (which includes 'removal' of data), and "unauthorised impairment of electronic

communication to or from a computer" (477.1). One can anticipate that the non-consensual use of spyware qualifies as accessing data without authorisation. Furthermore, as certain spyware products such as 'Cerberus' offers the opportunity to "wipe device memory", and spyware generally "impairs" the security of data "held on a computer" (476.2), the above stated offences could be relevant.

Stalking

Various types of legislation relating to stalking could also be applicable in the context of abusive use of spyware. For instance, Victoria's *Crimes Act 1958* has specific text supporting stalking convictions related to the offence of "causing an unauthorised computer function … in a computer owned or used by the victim or any other person" (21A(2)(bb)) and "tracing the victim's or any other person's use of the Internet or of e-mail or other electronic communications" (21A(2)(bc)). In this regard, Victoria has been anticipating technology-facilitated stalking, which is likely to also include the malicious use of spyware. Other states such as Queensland do not make specific reference to electronic monitoring or surveillance, but regard unlawful stalking as "following, loitering near, watching, or approaching a person", which can involve "contacting a person in any way, including … through the use of any technology" (Chapter 33A of the *Criminal Code Act 1899* QLD). A court would have to rule that the use of spyware was tantamount to 'following' and 'watching', in a fashion that caused the target to feel "apprehension or fear" and causes "detriment" to the stalked person. In such a circumstance the geo-locating functions of the spyware, for instance, could reasonably qualify as 'following'.

Breach of Confidence

In the absence of a tort for an invasion of privacy in Australia, the doctrine of 'breach of confidence' provides an option for civil action. Someone who has been targeted with spyware in a non-consensual context, could pursue the operator for sanctions related to 'breach of confidence' if it can be demonstrated that the "information is confidential", "the information was imparted in circumstances importing an obligation of confidence", and that "there has been an unauthorised use or threatened use of the information" (Office of the Information Commissioner Queensland 2019). It is conceivable that an individual targeted with spyware could convince a court that the unauthorised access and interception of their private phone data by the operator satisfies the above tests.

Other possible offences: intimidation, identity theft, fraud, property

Depending on unique fact scenarios regarding how the spyware was used and what functionalities the particular spyware product had, a variety of other possible offences could be committed by abusive spyware users. As mentioned earlier, some spyware products offer the capacity to send 'spoof' messages from the hijacked device. This could be reasonably understood as a violation of laws against impersonation. For instance, Western Australian law outlines that it is an offence for any person that "falsely represents himself to be some other person living or dead" if the intent is to "defraud any person" (Criminal Code Act 1913: s510). In the circumstances where a court is willing to accept that spoof messages are an intention to 'defraud', such an offence would be relevant.

Similarly, invasive spyware on someone's smart-phone scoops up a lot of sensitive data and

information about that person such that legislation relating to identity theft could be relevant. Using Queensland's *Criminal Code Act 1899* as an example, it is a misdemeanor to obtain "another entity's identification information for the purpose of committing, or facilitating the commission of, an indictable offence" (408D, (1)). This would include data that could potentially be captured by spyware including "the individual's passport or passport number", "the individual's financial account numbers, user names and passwords", or "information about the individual or the individual's relatives including name, address, date of birth, marital status and similar information" (408D, (7)). As contemporary use of smartphones often deal with logging into financial accounts, making flight reservations, and otherwise utilizing sensitive information, spyware products that deploy 'keylogging' features and tracks internet browsing activity could conceivably violate such identity theft legislation.

Similarly, 'image-based' abuse offenses are also relevant. A number of spyware products offer remote access to the cameras on the smartphone, allowing the ability to take pictures or video without the target being aware of the recording. As an example, New South Wales recently made it an offence to "record an intimate image without consent" and also an offence to "distribute an intimate image without consent" (see *Crimes Act 1900,* Division 15C, 91P and 91Q). Using spyware to capture photos and videos of a target could capture what would reasonably be regarded as "intimate" images. Likewise, as spyware-software shares the target's private data with the spyware vendor's servers and other third-party intermediaries, a court may rule that such a transmission of data counts as a form of distribution.

In the circumstances where the abuser has had to 'jail-break' or 'root' the device of the target without their consent, a further argument may also be considered concerning how this conduct is inherently an offence. For example, South Australian law has provisions against "Dishonest manipulation of machines" (see *Criminal Law Consolidation Act 1935,* Division 7, 141). In this context, it is an offence if a person "dishonestly manipulates a machine in order to – (a) benefit him/herself or another; or (b) cause a detriment to another". 'Jail-breaking' or 'rooting' a device to install spyware without the consent of the device's primary user would perhaps qualify as a 'dishonest manipulation of machines'. It is essential, however, that this offence not be more broadly misapplied to legitimate security research that might itself entail modification of digital devices.

The above highlighted laws are not an exhaustive guide to the potential offences committed when spyware is used abusively, but reflect the wide-variety of considerations created by spyware that has wide-ranging and significantly powerful capabilities of surveillance and manipulation over an individual's smart-phone. We provide a much more detailed analysis of consumer spyware and the Australian Privacy Act in a subsequent section of this report.

Technical Assessment of Consumer Spyware

Based on research conducted by project partners, HackLabs, and subsequent follow-on research conducted by researchers at Citizen Lab, this section of the report briefly summarises a number of technical characteristics specific to the operation of the sample spyware. Our primary findings reveal that:

- Many of the spyware apps included in this study have notable security issues and often take inadequate care of data during transit. The low quality security design of the spyware only increases the vulnerability of the personal data of those targeted by spyware. This raises additional risks of privacy violation beyond already existing pernicious social uses.
- Spyware is heavily reliant on the use of third-party intermediaries to execute their digital subscription delivery service. This information is useful to ascertain the degree of legal culpability, legal protections, regulations, and exposures across different jurisdictions. Our findings indicate that notable intermediaries are primarily located in the United States, Netherlands and Hong Kong.

In what follows, we illustrate the results of our findings as they relate to network activity, vulnerabilities in app security, and a brief discussion of the present status of anti-malware applications and their ability to detect spyware. It should be noted that the technical analysis described in this section is specific to spyware deployed on the Android operating system.

Consumer spyware often has significant security vulnerabilities

The design and operation of consumer spyware exhibited numerous weaknesses. In the technical analysis performed by this research, a number of significant vulnerabilities were discovered. In what follows, we briefly summarise the most significant vulnerabilities that were uncovered. For readers that might be interested in a more detailed technical analysis this information can be made available upon request.

TheTruthSpy

The overall security posture of TheTruthSpy application is very low. Security is lacking at all levels – from a network level protection of the backend servers, to the control panel web application, and also the API (Applications Programming Interface), which allows applications to communicate with one another. In particular, the application completely lacks encryption for data in transit between the devices and its backend servers. The application APIs lack authentication and only use easily obtainable device ID as the unique identifier, allowing different spoofing attacks, as well as allowing an attacker to register another arbitrary device for downstream control. The application's main web page is running outdated software with many known security problems. As a result of these security weaknesses, the additional privacy risks to targets, as well as to innocent parties whose data might be intercepted through the use of spyware, are significant.

Flexispy

One of the most significant security weaknesses in the Flexispy app is a lack of encrypted protocol for communications between the device and backend servers. While Flexispy was found to implement a custom encrypted binary protocol, it was found to work over HTTP port 80 which is not protected by the industry standard TLS protocol. While some messages are fully encrypted by Flexispy's custom protocol, others such as picture synchronisation only contain an encrypted header, leaving the associated content in plain text. Further research on Flexispy's update process found that the commands are sent without cryptographic protection, meaning that update processes in non-rooted phones are vulnerable to attack. Rooted phones may also be partially vulnerable to attack through the update process. The overall implication is that data can be exposed to the internet while in transit, rendering it vulnerable to malicious third-parties, and that hi-jacking the update process can allow an attacker to inject malicious code onto target devices.

Cerberus

The security posture of Cerberus is relatively better compared to the other apps in this project, however, the application exhibits several notable security deficiencies. Most notably in our research, we found that the API lacks endpoint authentication. As a result, messages and devices can be spoofed by malicious actors in order to exploit both operators, targets, and other individuals whose data might be collected through the use of the application.

mSpy and Teensafe (non-jailbroken iPhone)

The mSpy application, in contrast to all other examined applications, allows operation on a non-jailbroken device as well as on a jailbroken iOS device. Exfiltration of data through on iOS relies on, at a minimum, Apple ID credentials and the device passcode where relevant. Operating on a non-jailbroken device is possible because of the iCloud and iCloud Drive backup and storage mechanisms, which mSpy and Teensafe rely upon to present data to the user of spyware. Notably, owners of the Apple ID do not receive a notification that spyware might be mirroring data through iCloud and iCloud Drive backups. They may, however, receive a prompt to update their Apple ID password as a result of 'unusual' activity. While Apple does inform users when credentials are used on a new device or on the web, this feature is not present when accessing iCloud. Disabling of iCloud and iCloud Drive, as well as the sync mechanism, will interfere with the routine functioning of mSpy.

Network activity analysis reveals the commercial infrastructure that hosts spyware functionality

Analysis of the network activity of the apps in our sample ascertained the hosting environments and delivery services that make up the broader commercial infrastructure utilised by spyware companies. Examining the network activity also revealed the geographical transit points of data flows during the use of spyware, which is important for deducing relevant legal considerations that are specific to particular jurisdictions. Our network analysis involved monitoring data flows specific to IP addresses, as well as historical DNS data where relevant.

Table 2 Table of geolocation information associated with spyware applications

App	Domain	IP	Country	ASN Name	ASN #
Cerberus	www.cerberusapp.com	66.228.35.203	United States	Linode, LLC	63949
Flexispy	admin.flexispy.com	104.25.91.115	United States	Cloudflare, Inc.	13335
Flexispy	admin.flexispy.com	104.25.92.115	United States	Cloudflare, Inc.	13335
Flexispy	api.flexispy.com	180.150.144.84	Hong Kong	Rackspace IT Hosting AS IT Hosting Provider Hong Kong	45187
Flexispy	blog.flexispy.com	104.25.92.115	United States	Cloudflare, Inc.	13335
Flexispy	blog.flexispy.com	104.25.91.115	United States	Cloudflare, Inc.	13335
Flexispy	client.mobilefonex.com	180.150.156.198	Hong Kong	Rackspace IT Hosting AS IT Hosting Provider Hong Kong	45187
Flexispy	community.flexispy.com	104.25.91.115[DH1]	United States	Cloudflare, Inc.	13335
Flexispy	community.flexispy.com	104.25.92.115	United States	Cloudflare, Inc.	13335
Flexispy	ecom.flexispy.com	180.150.144.85	Hong Kong	Rackspace IT Hosting AS IT Hosting Provider Hong Kong	45187

App	Domain	IP	Country	ASN Name	ASN #
Flexispy	portal.flexispy.com	180.150.144.87	Hong Kong	Rackspace IT Hosting AS IT Hosting Provider Hong Kong	45187
Flexispy	push.mobilefonex.com	180.150.156.193	Hong Kong	Rackspace IT Hosting AS IT Hosting Provider Hong Kong	45187
Flexispy	www.flexispy.com	104.25.91.115	United States	Cloudflare, Inc.	13335
Flexispy	www.flexispy.com	104.25.92.115	United States	Cloudflare, Inc.	13335
mSpy	a.thd.cc	46.166.133.55[DH2]	Netherlands	NForce Entertainment B.V.	43350
mSpy	cp.mspyonline.com	104.25.84.24	United States	Cloudflare, Inc.	13335
mSpy	cp.mspyonline.com	104.25.85.24	United States	Cloudflare, Inc.	13335
mSpy	pipe.thd.cc	104.31.95.14	United States	Cloudflare, Inc.	13335
mSpy	pipe.thd.cc	104.31.94.14	United States	Cloudflare, Inc.	13335
mSpy	repo.mspyonline.com	104.25.85.24	United States	Cloudflare, Inc.	13335
mSpy	repo.mspyonline.com	104.25.84.24	United States	Cloudflare, Inc.	13335

App	Domain	IP	Country	ASN Name	ASN #
mSpy	thd.cc	104.31.94.14[DH3]	United States	Cloudflare, Inc.	13335
mSpy	thd.cc	104.31.95.14	United States	Cloudflare, Inc.	13335
mSpy	www.mspyonline.com	104.25.85.24	United States	Cloudflare, Inc.	13335
mSpy	www.myspy.com	104.20.20.58	United States	Cloudflare, Inc.	13335
mSpy	www.myspy.com	104.20.21.58	United States	Cloudflare, Inc.	13335
TheTruthSpy	my.thetruthspy.com	69.64.74.242	United States	Codero[DH4]	18501
TheTruthSpy	protocol-a735.thetruthspy.com	69.64.91.29	United States	Codero	18501
TheTruthSpy	protocol-a739.thetruthspy.com	69.64.91.29	United States	Codero	18501
TheTruthSpy	setupmail-a739.icloudappe.com	69.64.91.29	United States	Codero	18501
TheTruthSpy	thetruthspy.com	66.226.73.96	United States	Codero	18501
TheTruthSpy	www.thetruthspy.com	66.226.73.96	United States	Codero	18501

For unique IP addresses that were observed during the analysis, Cerberus and TheTruthSpy are exclusively located in the United States (Linode and Codero, respectively), Flexispy is 60% US-based (CloudFlare) and 38% Hong Kong-based (Rackspace), mSpy is 92% US-based (CloudFlare) and 8% Netherlands-based (NForce). The findings indicate that further investigation into relevant statutory obligation of intermediaries in each of these jurisdictions (the United States, Hong Kong, and the

Netherlands) is warranted. Moreover, intermediaries such as CloudFlare, Codero, Rackspace, Linode, and NForce should be further scrutinised for their role in the service provision of spyware for consumer audiences. Codero, it should be noted, has previously removed content relating to TheTruthSpy from their servers (Franceschi-Bicchierai 2019b).

Notes on the ability of Google Play Protect to 'discover' spyware

Evaluations of the protections afforded by Google Play Protect as a native anti-malware detection mechanism on Android devices, reveals that Google Play Protect provides a degree of protection from spyware applications. All versions of spyware in the technical sample (mSpy 5.30, FlexiSPY 3.0.1, Cerberus 3.5.3, and TheTruthSpy) were detected, apart from Cerberus, which is available in the Google Play store. However, in a subsequent round of testing in January 2019, TheTruthSpy was not detected. This is a mixed finding as it indicates that Google is taking some note of the risks posed by off-the-shelf spyware software. However, further evidence is needed to determine whether Google Play Protect is only blocking newer versions, and evidence exists that only minor code changes are required for spyware products to further circumvent Play Protect. This evasion, however, may only last a period of days before Google Play Protect detects these changes and subsequently re-identifies the spyware. More research is needed to systematically evaluate the latency between developer updates in spyware products and subsequent detection in Google Play Protect.

Part of the analysis of Google Play Protect also included a test to ascertain whether Google Play Protect was re-enabled on a device that had spyware already placed on it (in circumstances where Play Protect is required to be disabled for spyware installation, e.g. Hoverwatch), and whether detection of the spyware would subsequently occur. In all instances where Google Play Protect was re-enabled on a device that contained spyware, a prompt with an uninstall option would appear. Again, this finding suggests that enabling Google Play Protect on a device that contains spyware, and where Google Play Protect had been disabled, may be a partial method for identifying and removing unwanted spyware on non-rooted devices. It is important to note, however, that this finding is temporally specific, and may be subject to changes in both developer and Google practices. As such, these findings should be further tested.

Corporate Policy Assessments of Consumer Spyware Companies

This section reports on the analysis of relevant privacy policies and terms of service that are published by spyware companies. Privacy policies and terms of service are designed to inform customers about a company's obligations and commitments regarding data handling, security, and privacy. They also allow companies to outline an interpretation of their own liabilities with customers. These policies also routinely indicate what types of data are collected, how that data is classified (as personal information or not), and provide potential avenues for recourse that customers may have with the company regarding the use of their products and services.

In conjunction with researchers at the Citizen Lab and Ms Erica Vowles, we comprehensively examined spyware companies' corporate policy documents. We downloaded privacy policies, terms of service agreements and End User License Agreements (EULAs) for all of the spyware companies in our sample. Those documents were then subjected to analysis using a structured question set. Our lines of inquiry centred on:

- **How a company developed its privacy policy:** e.g., asking whether "there is a link to the privacy policy on the company's homepage," "whether there are references to compliance with: National privacy laws, international guidelines, self-regulatory instruments from associations?," and whether there is "a statement concerning which nation/court proceedings must go through?"
- **How companies addressed questions from users of the software, or those who are targeted by the software:** e.g., asking whether "there is a contact to a privacy officer listed?," whether "there is a description/discussion of who you can complain to if you're unsatisfied with the information/processes given by the organisation?," whether "there is a procedure for deleting information", or a "right to be forgotten"?
- **How a company captured personally identifiable information (PII):** e.g., whether "there are specific kinds of PII (ie, information about the 'users') collected?," "what types of categories are listed?" and whether there is "any distinction made between sensitive and non-sensitive PII?, and lastly "whether any distinction is made between information on children/adults?"
- **How a company secured personally identifiable information:** e.g., whether "commitments are made to the security of information?," whether "commitments are made about encryption/de-identification of data?," and whether "there is a note that users and/or government bodies will be alerted if a data breach occurs?"

Our findings suggest that spyware companies routinely failed to clearly indicate to targets how to have their data deleted in instances where abuse has occurred. Further to this absence, we also found that companies failed to include policies to notify persons that have been targeted by spyware in instances where a data breach might have occurred. And lastly, we found that companies also failed to account for the scope of personally identifiable information that is captured during routine operation of the software, which undermines the inherent purpose of privacy policies as an instrument that is designed to transparently disclose what, and how much, data is collected through

the course of the software's use. Likewise, our analysis of the privacy policies and terms of service reveals that they are disproportionately focused on the rights and guarantees that are afforded to the operators or purchasers of the software. Crucially, this ignores how the software can be misused, as well as how individuals might seek support from companies when they have been abused by their product.

Findings from analysing spyware company-policy documents

Each company provided access to privacy policies and terms of service from the homepage of their websites. Among these policies, many provided specific information about the jurisdiction in which potential disputes would be resolved. Overwhelmingly this referenced US-based courts, with specific state references to New York (Highster Mobile), Virginia (Hoverwatch), California (Teensafe) and Texas (TheTruthSpy). mSpy suggested an EU-based legal system with reference to the Czech Republic. Each company in our sample also explicitly noted that they reserved the right to change their privacy policies, however, Flexispy, Highster Mobile, and Mobistealth made no indication of when their policies were written or last updated. None of the companies provided historical versions of previous policies which would offer an understanding of how policies might have changed over time. Our examination of whether companies included relevant contact information, such as a privacy officer or other terms of service support staff, found that only three companies--Cerberus, mSpy, and TeenSafe--made explicit reference to dedicated privacy or legal contact support. Four other companies provided a generic email contact to receive questions, and only Mobistealth failed to provide any contact information in their policies.

While many of the companies offered support to correct or delete data, these overtures were directed to operators / purchasers of the software. More unclear is how targeted persons might go about contacting companies as a way to enquire about information collected about them, and how they might obtain access to, or request deletion of, this information. Given the extent to which spyware also collects the personal information of other third-parties that have communicated with the target, it is unclear how these individuals could activate their data access and correction rights under the Australian Privacy Act.

Our analysis also revealed that only a small cross-section of our sample - Cerberus, Hoverwatch, Mobistealth, Teensafe, and TheTruthSpy - explained the types of data that are collected from target devices. Any other reference to the collection of personally identifiable information (from Flexispy, mSpy, and Highster Mobile) was made in reference to visitors to their website or personal details that are collected at the point of commercial sale. Given that much of the marketing and promotion of spyware relates to parent-child monitoring, the collection of data on minors is recognised as a core business practice. However, Hoverwatch, mSpy, and Teensafe all stated that they do not knowingly collect data on children.

In spite of the security weaknesses noted in the technical section of this report, some spyware companies provided commitments about data security in their policies, while others made no comment regarding the security of personal information. Mobistealth specifically noted that they did not "manage" "nor control distribution of data, nor access personal data captured or stored on

servers and databases" that the company uses. Flexispy touted their "painstaking efforts to ensure that [this] data will be secure", in spite of being the subject of several major data breaches and a custom encryption protocol that transfers data in plain text (Francesco Bicchierai 2018). mSpy provided several details about their data handling practices, including third parties, information sharing, and data storage, but they too have been subject to serious data breaches in recent times (Krebs 2018). In instances where data breaches occur, only Cerberus and Highster Mobile indicated they would notify individuals, and mSpy noted they would notify both individuals as well as relevant data protection authorities. Most significantly, those who might be most negatively impacted by the use of the spyware--the targets of the malware--were never regarded as being important to be contacted in the event of a data breach. Furthermore, we found discrepancies between data location (premised on our network analysis) and jurisdictions that have been referenced in privacy policies, raising further confusion about the appropriate legal forum where disputes and remedies might be able to take place.

The Australian Privacy Act and Consumer Spyware

This section of the report summarises the most significant findings of the research project as it relates to Australia's chief information privacy framework--the Australian Privacy Principles (APPs) as enshrined in the Australian *Privacy Act (1988)*. The APPs lay out the obligations that government and businesses in Australia have when collecting, using, or disclosing information through the course of their commercial activities. The Office of the Information Commissioner (OAIC) is the government agency that is responsible for overseeing and enforcing the *Privacy Act (1988)* in a way that attempts to balance commercial interests with consumer privacy interests.

Are spyware companies accountable under the Australian Privacy Act?

Whether spyware companies are covered by the *Privacy Act (1988)* is largely dependent on two main factors. First is whether they have an annual financial turnover of 3 million dollars or more per year. For companies that operate outside of Australian jurisdiction, it can be difficult to ascertain their annual revenue. However, for any spyware companies that might have an annual turnover of less than 3 million dollars per year, the nature of their activities would appear to still bring them within the scope of the legislation. Entities that have an annual turnover of less than 3 million dollars per year are regarded as accountable under the Act if their activities are found to:

> "...disclose personal information about another individual for a benefit, service or advantage, or provide a benefit, service or advantage to collect personal information about another individual from anyone else, unless they do so with the consent of the individual or are required or authorised by or under legislation to do so."

Given that the personal information of prospective targets of the malware transit the server infrastructure of the companies themselves (where they are collected via the companies' products and services and subsequently made available to the operator via their online platforms and/or dashboards), they could be fairly regarded as engaging in activities that centre on the disclosure of personal information about individuals for a benefit, service, or advantage. Furthermore, given that many of the companies do not take adequate technical steps (such as push notifications) to acquire consent from targets of the spyware, they clearly do not engage in these activities through a meaningful consent regime. In fact, many of the apps in our study market and design their apps to be actively concealed from those that are targeted by them.

It is also clear that given the highly sensitive degree of the information collected through the use of consumer spyware, that data which is collected and disclosed through the use of spyware clearly meets the definition of personal information as defined under s.6 of the Privacy Act (ie, as "...information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable"). The information collected through the mobile apps could very easily meet the higher bar of 'sensitive information',

which imposes more stringent obligations under the Act. Sensitive information is defined under s.6 of the Act, as information or opinion about an individual's:

i) racial or ethnic origin
ii) religious beliefs or affiliations
iii) health information about an individual; or
iv) biometric information that is to be used for the purposes of automated biometric verification or biometric identification; or
v) biometric templates

The Australian Privacy Principles (APPs) and Consumer Spyware

Under *APP1* (titled, "Open and transparent management of personal information"), entities under the Act are required to "have a clearly expressed and up to date policy...about the management of personal information..." (APP1). These obligations include, but are not limited to, noting the types of information that is collected and held, how the information is collected and held, the purposes for which information is collected, held, used and disclosed, how an individual whose information has been collected may seek correction of the information, and how entities will deal with a breach. Our analysis of the companies' privacy policies suggests that consumer spyware companies' compliance with *APP 1* is patchy and inconsistent. Companies routinely failed to account for the scope of information they collected and held. The overwhelming majority failed to be explicit about how they collect and hold information, with Mobistealth even explicitly mentioning that they do not "manage" or "control" their own data handling practices. Moreover, companies overwhelmingly failed to mention the purposes for which personal information is collected *unless* it was specific to the collection of personal information for the purposes of commercial transactions (ie, to process payment with customers that will be deploying the spyware). Glaringly absent was mention of the collection of sensitive personal information from targeted persons or other affected third-parties through the use of the spyware itself.

Furthermore, while three companies noted that individuals could contact a dedicated support person for assistance with privacy issues (Cerberus, mSpy, and TeenSafe), the majority provided a generic email address for asking general questions. Mobistealth failed to provide any contact information whatsoever regarding their policies. Insofar as companies are required under *APP1* to disclose how entities will deal with a breach, only Cerberus and Highster Mobile mentioned they would contact affected individuals. It was unclear whether these individuals referred to the 'operator' or 'target' of the malware. Only mSpy noted that they would notify both individuals as well as relevant data protection authorities. Six other companies failed to make any mention about data breach notifications and responses. Under Australia's mandatory notifiable data breach scheme (*Privacy Amendment (Notifiable Data Breaches) Act 2017)*, only mSpy would be considered compliant.

Under *APP3.3*, entities must not collect sensitive information about an individual unless the individual consents to the collection of that information. While consumer spyware companies attempt to delegate the issue of consent to the operators of their software in the End-User License

Agreements (EULAs), many also actively seek to render their products invisible to those whose sensitive personal information is being exploited. In both instances, consumer spyware companies would appear to be in breach of *APP3* through their inability to maintain a lawfully sufficient consent regime. Furthermore, for third-parties whose information has been collected for no other reason than because they have been in communication with a target, there is also no practical way that consent could be given. Finally, these problematic realities of data collection through consumer spyware must also be squared with *APP3.5*, which states that "An APP entity must collect personal information only by lawful and fair means." Given these many shortcomings, it would appear unlikely that collection performed through consumer spyware in its current manifestation would constitute either lawful or fair means under the Privacy Act.

Entities under the Privacy Act are obligated to take reasonable steps to notify individuals about the collection of their personal information at or before the time it is collected, where it is practicable to do so (*APP 5*). This obligation extends to include instances where information is collected on someone other than the individual that has consented to the primary collection. *APP 5* is explicit that this obligation applies *especially* in instances where "the individual may not be aware that the APP entity has collected the personal information" (APP 5.2 (ii)). In the context of spyware, this obligation places clear requirements upon consumer spyware companies to "ensure that the individual is aware of such matters", and to acquire consent from the owner of targeted devices prior to operation. At the time of writing, the consumer spyware companies in this study appear to be in clear contravention of *APP 5*.

APP 11 further obligates entities that manage personal information through the course of their operations under the Privacy Act to take reasonable steps to protect this information "from misuse, interference, and loss; and...from unauthorised access, modification or disclosure.'' (*APP 11.1* (a) and (b)). In recent years, there have been several instances where consumer spyware companies have suffered serious data breaches. When this track record is combined with the results of the numerous security weaknesses revealed through the course of our technical analysis, it could be argued that consumer spyware companies may be failing to meet their obligations to protect information from misuse, interference, and loss. However, it bears mentioning again that consumer spyware companies uphold practices that themselves facilitate the interference, loss, misuse and/or unauthorised disclosure of personal information as a core part of their business model.

This brief summary identifies a number of issues and concerns regarding the compliance (or relative non-compliance) of consumer spyware companies under the Privacy Act as outlined in the APPs. A key follow-on concern therefore becomes the enforcement powers of relevant regulatory bodies. In the event that a breach of the Privacy Act has occurred, the OAIC has powers to investigate potential interferences with privacy on the basis of a formal complaint made by an individual. Generally speaking, the OAIC will attempt to mediate and reconcile the infringements on the basis of a complaint, however, they also have powers to impose civil penalties for activities that exceed 'minor' or 'inadvertent' contraventions and which amount to 'serious' and 'repeated' interferences (Chapter 6 of the Privacy Act 1988; 6.13). Section 6.24 lays out the relevant factors to be considered when determining what constitutes a serious interference with privacy, including:

- the number of individuals potentially affected
- whether it involved 'sensitive information' or other information of a sensitive nature

- whether significant adverse consequences were caused or are likely to be caused to one or more individuals from the interference
- whether vulnerable or disadvantaged people may have been or may be particularly adversely affected or targeted
- whether it involved deliberate or reckless conduct
- whether senior or experienced personnel were responsible for the conduct. (s. 6.24)

These serious interferences can be considered 'repeated' if they entail the same or different acts on two or more occasions, which together can indicate that an entity is chronically disregarding its obligations to uphold privacy as defined through the APPs. For the OAIC to make an overall determination, it will consult factors laid out in paragraph 38 of the Privacy regulatory action policy.

The evidence presented through the course of this research project raises serious questions about whether the activities of consumer spyware companies facilitate persistent and ongoing serious interferences with privacy. With pending legislation to be introduced in the latter half of 2019 that would enhance the OAIC's powers of enforcement to include stronger administrative monetary penalties, a significant opportunity to reform the Privacy Act could help rein in the more pernicious practices of consumer spyware companies. It is imperative, in our view, that these proposed amendments move beyond mere consideration of the privacy violations of social media platforms to include consumer spyware, particularly as these new rules are expected to explicitly consider rules that would specifically protect the personal information of children and other vulnerable groups--those that are most significantly impacted through the use of spyware.

Conclusions

The risks posed by consumer spyware are many. Spyware can provide extensive visibility into the most personal and sensitive activities of those that are targeted by it. For this reason, it is often used to facilitate controlling and abusive behaviours that can result in serious psychological, emotional, social, and financial harms. The documented risks of technology-facilitated abuse, harassment, and violence through the use of consumer spyware are further compounded by a range of risks associated with data privacy, resulting from illicitly collected information, an absence of a meaningful consent regime, and weak data security practices.

Regrettably, many of the companies reviewed in this study design and market their products in ways that predictably result in these unfortunate outcomes. In spite of this, companies included in this study failed to provide explicit assistance and support for those that may be negatively impacted through the use of their products. Beyond the companies themselves, there also exists a broad ecosystem that includes third-party intermediaries that help to deliver powerful spyware capabilities to general consumer audiences. The detail provided in this report raises serious alarm about a disconcerting number of risks that consumer spyware poses for the safety, security, and privacy of Australians, particularly for women and children.

While a number of legal and regulatory enforcement possibilities currently exist in Australia that might help to minimise the harms brought about through this largely unregulated industry, greater awareness and education is needed to spur meaningful attempts toward enforcement. One of the more notable examples of an enforcement gap in our study relates to the accountability spyware vendors have under Australia's Privacy Act. Our analysis shows that spyware vendors are likely to be operating in clear violation of Australia's data privacy framework. While the enforcement of existing legal and regulatory measures is important, there is, however, further demand for legal and policy reform to mitigate harms associated with this largely unregulated and damaging industry. In the following section we make concrete recommendations to this end, on the basis of our findings in this report. Perhaps most importantly, however, is a vital reminder that any implementation of the recommendations found in this report is not enough in itself. While legal, technical, and policy reforms are significant and much needed, they must also be accompanied by a broader societal response that addresses systemic gender inequalities, misogyny and corrosive values that exist as root causes to all forms of technology-facilitated harassment, abuse, and violence which are disproportionately directed at women, non-binary persons, and children.

Recommendations

After reflecting on all of the findings of this research, we suggest that combating the threat of abusive spyware will require multiple strategies:

Recommendation 1

'Offensive actions' to disrupt the operations of the consumer spyware industry will be difficult given the cross-jurisdictional legal issues (as identified in this report). However, pressure can be placed on some of the identified commercial actors that host or facilitate spyware products. This includes the intermediaries identified in our technical analysis.

Recommendation 2

In the short-term, Google should take steps to remove 'Cerberus' from their Play Store. In the longer-term, they should take further steps to ensure similar 'stealthy' apps that have significant abusive potential are not hosted on their Play Store.

Recommendation 3

There are many options for 'defensive actions' that can be taken to protect consumers from malicious spyware. This can include information awareness on the threat of spyware and promoting an understanding of how consumer spyware functions. For example, that it can only be installed on someone's phone if the operator has physical access to the device. Likewise, certain steps can be taken to identify if they have been compromised by spyware. See the materials that we produced for the Women's Services Network (WESNET 2019 – Appendix A) for further details.

Recommendation 4

Law enforcement and public authorities should escalate their attention and focus on the threat of spyware. Australian bodies can enforce many of the existing forms of legislation that address the abusive use of consumer spyware, notably those found under the Privacy Act. We have detailed numerous instances for potential enforcement of existing powers that relate to existing obligations that could be imposed on spyware companies.

Recommendation 5

Protections against abusive use of spyware in Australia would also be better served by improvements to general legal protections for privacy in Australia. The introduction of a tort for an invasion of privacy in Australia would be an important development toward this end. Moreover, impending amendments to the Privacy Act should consider the novel threat posed by the spyware industry as documented in this report. Broadening the regulatory toolkit of the OAIC, such as enhanced administrative monetary penalties and, enhanced data protection obligations for especially vulnerable segments of society, may help to minimise the persistent privacy interferences associated with consumer spyware companies.

Recommendation 6

More research and support tools are required to improve on-device scanning for spyware, and perhaps, forms of network-traffic analysis that detect the presence of spyware. This can help address ambiguity for those who believe they are targeted by spyware by technically identifying spyware's presence or absence. Major technology companies should continue to implement product changes that mitigate the surreptitious functioning of consumer spyware. This could, for example, include protections to help prevent the surreptitious installation and operation of spyware that rely on insecure channels to update applications.

Authors

Dr Adam Molnar

Dr Adam Molnar is currently Assistant Professor in the Department of Sociology and Legal Studies at the University of Waterloo. He recently returned to Canada from Australia, where he was a Lecturer in the Department of Criminology at Deakin University for the duration of this project. His research interests focus on questions of privacy and social control that emerge at the intersections of technological innovation, surveillance, and policy/law.

Dr Diarmaid Harkin

Dr Diarmaid Harkin is an Alfred Deakin Postdoctoral Research Fellow at Deakin University based in the Alfred Deakin Institute. He has recently written a book on private security companies that work with domestic violence services, *Private Security and Domestic Violence* (Routledge). His other active research interests include the challenges of cyber-policing and the consumer spyware industry.

Appendix A – Risk-response materials produced from this research hosted by WESNET

Full link: https://techsafety.org.au/wp-content/uploads/2019/05/TSA_HDT-Mobile-Spyware_V2.1.pdf

WESNET
The Women's Services Network

MOBILE SPYWARE

Please note that the contents of this document should not be regarded as legal advice. The information contained within is relevant as of December 2018.

Safe phone/device

When searching for information or calling for support we recommend using a phone/device you do not suspect is monitored. This could be a public library, support worker or a trusted family member or friend's phone or computer.

National Sexual Assault, Domestic and Family Violence Counselling and Information – 1800 RESPECT

If you suspect someone is monitoring you using technology, the abusive person may also be making you feel unsafe in other ways. If you would like to explore support options available, you can contact 1800 RESPECT by phone (1800 737 732) or online chat (24 hours) from a safe phone or device. If you have a support worker, it may be helpful to discuss the monitoring and technology abuse with them and incorporating into your support and safety plan.

Safety Planning

Before taking action please consider how the person may react if you remove their ability to monitor you. You may wish to discuss this with a support worker and incorporate removing access into your safety plan.

I am concerned that spyware is on my phone. Is this possible?

For spyware to have been placed on your phone, someone would have needed physical access to the device.

(Note: It is *EXTREMELY UNLIKELY* for someone to be capable of placing spyware onto your phone without having physical access to the actual device. There are known examples of spyware that is used by government or national intelligence agencies that can be installed remotely. Such capabilities are extremely rare, cost hundreds of thousands of dollars, and are unlikely to be available to the vast majority of people. Therefore, the possibility of spyware being present on your phone can be largely discounted if no one had physical access to your device).

If someone did have physical access to your phone, and they knew your passcode, it is *conceivable* that spyware may have been placed on your phone. This article however, will help you identify whether that is *likely*, and what steps can be taken to help identify and potentially remedy possible threats.

What is spyware and what can it do?

This document considers "mobile spyware" to refer to an app or program that is deliberately placed on someone's mobile device for the purpose of monitoring that person.

Depending on the type of spyware installed, in most cases, mobile spyware will monitor:

- Call history, including phone number, date, and length of call
- Text messages, including phone number and SMS content
- Contacts
- Internet browsing, including history and bookmarks
- Location of the phone
- Photos taken on the phone
- Email downloaded onto the phone

Mobile Spyware | Last updated April 2019 V2.1
www.techsafety.org.au • techsafety[at]wesnet.org.au

If the phone has been jailbroken (iPhone) or rooted (Android), spyware software can monitor more, including:

- Certain messaging apps, such as WhatsApp, Viber, Skype
- Phone conversations
- Using the phone's microphone to record the phone's surrounding

It is difficult to identify whether spyware has been installed, since most spyware products operate in "stealth" mode, so it cannot be detected on the phone.

Once the software is installed, the abusive person can monitor all the above activity via an online website.

If it's not spyware, what else could it be?

There are several methods by which a person can track or monitor the activities of another person using technology other than Spyware. Monitoring information on Facebook, for example. Similarly, if a person can login to the iCloud or Google account associated with the phone, information from the phone can be accessed that may include location information. Many phones have functions such as "Find My Phone" that can be used to locate the owner of the phone. Within the context of this document, we do not consider these to be "spyware". It is recognised, however, that these can be a problem from the perspective of tracking and stalking. For information on how to address those issues, please see information available in the WESNET Women's Technology Safety and Privacy Toolkit. [www.techsafety.org.au/resources]

I own an iPhone. What are the risks of spyware on iPhones?

If you have an iPhone 6 or higher and have been regularly updating the iOS (operating system), the likelihood of spyware being on your phone without your knowledge is EXTREMELY UNLIKELY.

If you have an older iPhone model, or have not been updating your iOS on a regular basis, the likelihood of spyware being on your phone without your knowledge is still largely unlikely (but not impossible). In this circumstance the risk of spyware being on your iPhone without your knowledge is only a *credible* possibility if (a) someone had physical access to your device, (b) that person was aware of your device passcode, as well as your Apple ID login and password.

If you are in the circumstance whereby another person does have access to your physical device, your device passcode, as well as Apple ID login details, and you have reason to believe spyware is on your device, please contact WESNET from a safe device for further information on spyware. [email techsafety@wesnet.org.au]

I own an Android. What are the risks of spyware on phones that use the Android operating system?

(This includes phones by Samsung, Sony Xperia, Google Pixel, Huawei, LG, HTC, Nokia, etc)

The Android operating system is more vulnerable to spyware being placed on someone's device without their knowledge compared to iPhone. Unfortunately, it is also easy for a non-expert user to conceal traces of spyware on Android devices. If you are in the circumstance whereby another person does have access to your physical device, your device passcode, and you have reason to believe spyware is on your device, please contact WESNET from a safe device for further information on spyware.

Can I take my phone to the shop where it was purchased or to a local 'tech expert' to check for spyware?

There are certain forms of spyware that could be easily identified by an in-store, consumer retail outlet 'tech expert'. But there are also forms of spyware that would require a more forensic examination that is not readily available to individuals who work in computer or smartphone stores.

Depending on your situation, if the stalking/surveillance through spyware is just one part of the abuse you are experiencing you may wish to seek support from a family violence service to put a safety plan in place, or you may want to contact 1800Respect for advice.

I have strong reasons to believe that spyware is being used against me right now. What can I do right now to protect myself?

If you do not have the time or opportunity to seek support regarding spyware, but have STRONG reasons to believe that spyware is tracking you, there are some provisional, emergency steps you can take to protect yourself.

- Consider using another phone or device for communication or other activities (such as searching for support services) that you would like to keep private. Continuing to use the phone in this way can be helpful if you do not want the abusive person to know that you suspect spyware is on the phone.
  (Note: As a precaution, we recommend having conversations (on another device or in-person) that you would like to keep private, out of earshot of the device as some spyware may be able to record the surroundings of the phone).
- Also keep in mind that spyware can monitor location, so you may want to be careful about where you go with the phone. If you take the phone to the police, the abuser may know that the phone is at the police station, for example, so think through of any safety issues that you might need.
- Spyware will only communicate information whilst the phone is turned on and is connected to the internet. Therefore, turning off the phone will allow temporary relief from GPS tracking or any danger of the camera capturing pictures, audio, or video.
  - (Note: Turning on 'Airplane mode' is also likely to temporarily prevent the spyware from tracking your phone. However, there are rare circumstances under which 'Airplane mode' can be faked and the phone may still be tracking your data despite being in 'Airplane mode').
- If it is safe to do so, performing a factory reset on your device, ensuring the operating system is up to date and changing your Apple ID/iCloud or Google login passwords might rid the device of the spyware. This will work for many types of spyware but not all. (Hence why seeking further information from WESNET is advisable). A family violence support service will be able to assist you with considering if you would like to preserve evidence, how the abusive person might react if you remove their ability to monitor you, and help you develop a safety plan.
- As a measure of last resort, purchasing a brand-new phone should remove the threat of spyware. (However, if purchasing a new Android device, avoid automatically reinstalling apps from your app library and see additional settings below). Your new device should be free of spyware, but it is strongly advisable to change your iCloud/Apple ID or Google login passwords.
  - (Note: On Android phones, check the security settings and disable "allow installation from unknown sources" and select "verify apps" to assist in preventing spyware from being installed).

Grateful Acknowledgement

This information has been compiled by three researchers, Dr Diarmaid Harkin, Dr Adam Molnar and Ms Erica Vowles, who spent several months testing spyware apps on Android and Apple phones, in order to determine what level of surveillance such apps enable, and the threat posed to phone users. This information is up to date as of December 2018. This document was developed in conjunction with representatives from WESNET and funded by ACCAN. *The operation of the Australian Communications Consumer Action Network is made possible by funding provided by the Commonwealth of Australia under section 593 of the Telecommunications Act 1997. This funding is recovered from charges on telecommunications carriers.*

Read this article for more information on Android phone privacy and security.
Read this article for more information on iPhone privacy and security.
Read this article for more information on Smartphones and location strategies
Read this handout for Computer Spyware and Safety

Glossary

Definitions of terms commonly used in this document are contained here.

Android	A mobile-phone operating system developed by Google
API	Application Programming Interface. A set of protocols that allow Applications to communicate with one another.
APP	Australian Privacy Principles
ASN	Autonomous System Number. Supports routing functionality on the internet.
DNS	Domain Name System. The 'phonebook' of the internet.
Domain	An administrating host of internet communication and functions.
HTTP	Hypertext Transfer Protocol. The protocol used for communication on the internet.
iOS	An operating system developed by Apple.
IP	Internet Protocol. A unique identifier for internet communication.
SMS	Short Message Service used to transmit messages between phones
TLS	Transport Layer Security. A protocol used for secure communication over the internet.
VoIP	Voice over Internet Protocol. The technology behind internet video-calls.

References

Brewster T (2016) Everything We Know About NSO Group: The Professional Spies Who Hacked iPhones With A Single Text. *Forbes*. Available online: https://www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/#71c94a4b3997

Burkart P and McCourt T (2017) The international political economy of the hack: A closer look at markets for cybersecurity software. Popular Communication 15(1): 37-54.

Citron D K (2015) Spying Inc. Washington and Lee Law Review 72(3): 1243-1282.

Cottle M (2014) The adultery arms race. The Atlantic. Available online: https://www.theatlantic.com/magazine/archive/2014/11/the-adultery-arms-race/380794/ (accessed 30th April 2018)

Cox J (2017) I Tracked Myself With $170 Smartphone Spyware that Anyone Can Buy. Vice: Motherboard. Available online: https://motherboard.vice.com/en_us/article/aeyea8/i-tracked-myself-with-dollar170-smartphone-spyware-that-anyone-can-buy (accessed 26th April 2018).

DOJ (2014) Man Pleads Guilty for Selling "StealthGenie" Spyware App and Ordered to Pay $500,000 Fine. The United States Department of Justice. Available online: https://www.justice.gov/opa/pr/man-pleads-guilty-selling-stealthgenie-spyware-app-and-ordered-pay-500000-fine (accessed 26th April 2018).

Franceschi-Bicchierai L (2019a) This Spyware Data Leak Is So Bad We Can't Even Tell You About It. Vice: Motherboard. Available online: https://www.vice.com/en_us/article/j573k3/spyware-data-leak-pictures-audio-recordings

Franceschi-Bicchierai L (2019b) Hosting Provider Finally Takes Down Spyware Leak of Thousands of Photos and Phone Calls. Vice: Motherboard. Available online: https://www.vice.com/en_us/article/7xnybe/hosting-provider-takes-down-spyware-mobiispy

Franceschi-Bicchierai L (2018) A Hacker Has Wiped a Spyware Company's Servers— Again. Vice: Motherboard. Available online: https://motherboard.vice.com/en_us/article/3k7a5k/ hacker-wipes-spyware-retina-x-flexispy (accessed February 16, 2018)

Franceschi-Bicchierai L and Cox J (2017) Inside the 'stalkerware' surveillance market, where ordinary people tap each other's phones. Vice: Motherboard. Available online: https://motherboard.vice.com/en_us/article/53vm7n/inside-stalkerware-surveillance-market-flexispy-retina-x (accessed 22nd May 2018)

Harkin D, Molnar A, and Vowles E (2019) The commodification of mobile phone surveillance: An analysis of the consumer spyware industry. *Crime Media Culture.* Available online: https://journals.sagepub.com/doi/full/10.1177/1741659018820562 (accessed 3rd July 2019).

Hern A (2015) Hacking Team hacked: firm sold spying tools to repressive regimes, documents claim. The Guardian. Available online: https://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim (accessed 26th April 2018)

Krebs B (2018) For 2nd Time in 3 Years, Mobile Spyware Maker mSpy Leaks Millions of Sensitive Records. Krebs on Security. Available online: https://krebsonsecurity.com/2018/09/ for-2nd-time-in-3-years-mobile-spyware-maker-mspy-leaks-millions-of-sensitive-records/ (accessed 4th September 2018)

La Rue (2013) Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. UN General Assembly Human Rights Council. Available online: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (accessed 22nd May 2018)

Lakhani N (2018) UK sold spyware to Honduras just before crackdown on election protesters. The Guardian. Available online: https://www.theguardian.com/world/2018/feb/08/uk-sold-spyware-to-honduras-just-before-crackdown-on-election-protesters (accessed 26th April 2018).

Lyons K (2018) Stalkers using bugging devices and spyware to monitor victims. The Guardian. Available online: https://www.theguardian.com/uk-news/2018/feb/13/stalkers-using-bugging-devices-and-spyware-to-monitor-victims (accessed 1st May 2018).

Marczak B, Scott-Railton J, and McKune S (2015a) Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware. The Citizen Lab. Available online: https://citizenlab.ca/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/ (accessed 26th April 2018)

Marczak B, Scott-Railton J, Senft A, Poetranto I, and McKune S (2015b) Pay No Attention to the Server Behind the Proxy Mapping FinFisher's Continuing Proliferation. The Citizen Lab. Available online: https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/ (accessed 26th April 2018)

Marczak B and Scott-Railton J (2016) The Million Dollar Dissident NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender. The Citizen Lab. Available online: https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/ (accessed 26th April 2018)

McKune S and Deibert R (2017) Who's watching little brother? A checklist for accountability in the industry behind government hacking. The Citizen Lab. Available online: https://citizenlab.ca/wp-content/uploads/2017/03/citizenlab_whos-watching-little-brother.pdf (accessed 22nd May 2018)

Office of the High Commissioner of Human Rights (2019) Convention on the Rights of the Child. Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989 entry into force 2 September 1990, in accordance with article 49. Available online: https://www.ohchr.org/en/professionalinterest/pages/crc.aspx

Office of the Information Commissioner Queensland (2019) Breach of Confidence. Available online: https://www.oic.qld.gov.au/annotated-legislation/rti/schedule-3/8-information-disclosure-of-which-would-found-action-for-breach-of-confidence/section-81/breach-of-confidence#footnote1

Parsons C, Molnar A, Dalek J, Knockel J, Kenyon, M, Haselton B, Khoo C, and Deibert R (2019) *The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry*. Citizen Lab. Available online: https://citizenlab.ca/2019/06/the-predator-in-your-pocket-a-multidisciplinary-assessment-of-the-stalkerware-application-industry/ (accessed 28 June 2019)

Privacy International (2018) https://www.privacyinternational.org/search/node?keys=spyware (accessed 26th April 2018)

Timberg C and Zapotosky M (2014) Maker of StealthGenie, an app used for spying, is indicted in Virginia. *The Washington Post.* Available online: https://www.washingtonpost.com/business/technology/make-of-app-used-for-spying-indicted-in-virginia/2014/09/29/816b45b8-4805-11e4-a046-120a8a855cca_story.html?noredirect=on&utm_term=.7965d448725c (accessed 26th July 2019)

Universal Declaration of Human Rights (2019) *United Nations.* Available online: https://www.un.org/en/universal-declaration-human-rights/ (accessed 3rd July 2019)

Valentino-De Vries J (2018) Hundreds of apps can empower stalkers to track their victims. The New York Times. Available online: https://www.nytimes.com/2018/05/19/technology/phone-apps-stalking.html?smtyp=cur&smid=tw-nytimes (accessed 22nd May 2018)

Victoria Legal Aid (2019) Conditions in a family violence intervention order. Available online: https://www.legalaid.vic.gov.au/find-legal-answers/family-violence-intervention-orders/conditions-in-family-violence-intervention-order

WESNET (2019) *Mobile Spyware: Identification, Removal, and Prevention.* Available online: https://techsafety.org.au/resources/resources-women/mobile-spyware-identification-removal-prevention/ (accessed 3rd July 2019)

Whittaker Z (2018) Teen phone monitoring app leaked thousands of user passwords. ADNET. Available online: https://www.zdnet.com/article/teen-phone-monitoring-app-leaks-thousands-of-users-data/

Women's Aid (2018) Online and digital abuse. Available online: https://www.womensaid.org.uk/information-support/what-is-domestic-abuse/onlinesafety/ (accessed 1st May 2018).

Legislation

Crimes Act 1900 (NSW)

Crimes Act 1958 (Victoria)

Criminal Code Act 1899 (QLD)

Criminal Code Act 1913 (WA)

accan

The Consumer Spyware Industry

An Australian-based analysis of the threats of consumer spyware

Criminal Code Act 1995 (Commonwealth)

Criminal Law Consolidation Act 1935 (SA)

Family Law Act 1975 (Commonwealth)

Privacy Act 1988 (Commonwealth)

Privacy Amendment (Notifiable Data Breaches) Act 2017

Surveillance Devices Act 1999 (Vic)

Telecommunications Offences and Other Measures Act 2004 (Commonwealth)