Check for updates

Article

CMC

Crime Media Culture
1–28
© The Author(s) 2019
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/1741659018820562
journals.sagepub.com/home/cmc
SAGE

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

Diarmaid Harkin
Deakin University, Australia

Adam Molnar
Criminology, Deakin University, Australia

Erica Vowles
Melbourne, Australia

Abstract

This article examines the attempts of 'spyware' developers to commodify and market their products to a general audience. While consumers of 'spyware' have often been government and law enforcement (Citizen Lab, 2015), there is an increasing attempt to market, sell, and commodify 'spyware' for use by wider audiences. 'Spyware' is sold as a security product commonly aimed at businesses, parents, and intimate partners. Pursuant to calls for a "sociology of security consumption" (Goold et al., 2010: 3), this article analyzes how nine prominent spyware vendors attribute meaning to their products. Spyware vendors face particularly fraught marketing challenges as the general deployment of spyware: a) is often utilized in forms of intimate partner abuse; b) is "morally troubling" from the perspective of being corrosive to many forms of social relations (Loader et al., 2014: 469); and c) has limited contexts where it could be deployed without violating surveillance laws. More specifically, this article compares the social meaning that vendors attempt to give to spyware and contrasts this with the powers of surveillance provided by the product, the marketing messages that appear to support non-consensual use, and the lack of guidance for non-consenting spyware targets to have recourse with the vendors.

Keywords

Family violence, privacy, private security, spyware, surveillance

Corresponding author:
Diarmaid Harkin, Deakin University, 221 Burwood Highway, Burwood, Melbourne, Victoria, 3125, Australia.
Email: diarmaid.harkin@deakin.edu.au

Introduction

There is a growing commercial availability of significantly invasive tools of surveillance known as 'spyware'. Although widely used as a tool of espionage to be deployed by nation-states and law enforcement, spyware is also increasingly packaged and sold to a general-use audience who may wish to place mobile phones, tablets, or personal computers under observation. Commercially-available spyware offers significant powers of surveillance over a target, with typical software offering the ability to remotely collect text messages, phone conversations, real-time GPS location data, and internet browsing data, and to activate the microphone or camera of the target device (Cox, 2017). Furthermore, a number of spyware vendors provide monitoring of WhatsApp messages, online dating applications, and personal images and videos, and use keylogging functions to reveal passwords of targets for approximately US$100 per month (using the example of 'MSpy').

Powerful and cheap spyware is thus readily available for a mass audience facilitated by a growing industry that encompasses a wide variety of vendors, often using professional and glossy websites with 24/7 call centre technical support (Franceschi-Bicchierai and Cox, 2017). Of interest in this article, however, is how the commercial use of spyware is subject to a process of commoditization that attempts to frame the meaning of the software and create norms around its use. Placing the commodification of spyware for consumer audiences under scrutiny, this article subjects a sample of nine vendors to a "sociology of security consumption" (Goold et al., 2010: 3), examining the process of how companies attempt to give meaning to their product as a 'legitimate' item of trade. Spyware vendors face a number of notable challenges in legitimizing their products. Firstly, spyware is associated with a wide range of human rights abuses perpetrated by governments (McKune and Deibert, 2017; Marzcak et al., 2015a, 2015b). Furthermore, it is increasingly utilized in forms of intimate partner abuse, with groups advocating on behalf of those subject to family violence being increasingly vocal on the impact of commercially available spyware on their clients (see for example Lyons, 2018; Re:Charge, 2015; Southworth, 2014: 3; Women's Aid, 2018). Secondly, it is also what Loader et al. (2014: 469) would refer to as a "morally troubling" product that can be viewed as culturally and morally corrosive to forms of social relations including parental-child relationships, industrial relations, personal privacy, and the general integrity of digital communications. And thirdly, the use of spyware as a tool of surveillance typically faces a number of legal restrictions on its manufacture and use (Citron, 2015). The 'legitimate' use of spyware is either confined to law enforcement or in circumstances where both parties – the target and the operator – agree and consents to its implementation. However, in many jurisdictions it is illegal to intercept private communications without the knowledge of the target, therefore spyware can only be legitimately deployed in a narrow number of circumstances.

Despite such limitations and challenges, spyware is widely available for consumption and this article aims to scrutinize and critique how vendors market and frame their product. Certain vendors such as 'TeenSafe' strongly emphasize that the product is for consensual monitoring of children by parents, while others suggest the spyware should be used for employee monitoring or anti-theft purposes. Other vendors of spyware have also openly marketed their product as a tool to surreptitiously monitor intimate partners (Armageddon, 2017; Franceschi-Bicchierai and Cox, 2017). Due to the scope for abuse, damage, and malicious intimidation inherent within the capabilities of the software, it is thus crucial to critically assess the process of 'meaning-making' and

marketing around spyware. As will be shown, while spyware products can often be largely similar in terms of the type of data captured and the underlying functionality, vendors take varying approaches to package, brand, and market their software in ways that minimize or conceal the more morally troubling aspects of their product.

This article therefore proceeds over six steps. The first step will briefly outline an overview of the 'spyware industry' that variously services clients such as nation states, law enforcement, and also general consumer audiences. Second, the risks and damage caused by spyware will be outlined with a particular focus on its impact in the context of family violence. Third, we argue that spyware ought to be subject to a "sociology of security consumption" (Goold et al., 2010: 3) to unpack how this product is reimagined for general consumer use. Fourth, the methods for how nine spyware vendors were selected for sampling and subject to closer semiotic analysis will be described. Fifth, a number of observations will be reported on how spyware is commodified, such as the tensions between 'small print' legal disclaimers that emphasize consensual use and more prominent marketing claims that sometimes promise 'undetectable' or 'hidden' implementation. And finally, a larger discussion will be considered reflecting on the morally ambiguous and often troubling aspects of the commodification of powerful spyware and the need for more social, political, legal, and academic scrutiny of this burgeoning industry.

Spyware: An overview of a burgeoning industry

There are difficulties in attempting to provide a comprehensive history of the spyware industry or to establish a clear understanding of the scope and span of the range of its producers, consumers, and products. What we do know about the spyware industry largely comes from hacked or leaked data (such as in the case of the spyware vendors 'Hacking Team' whose internal documents were made public; see Hern, 2015), or the work of research centres such as 'The Citizen Lab' (McKune and Deibert, 2017), advocacy groups such as Privacy International (Privacy International, 2018), and investigative reporting (see for example Cox, 2017; Valentino-DeVries, 2018). Legal proceedings against spyware producers have also been rare (although, there are exceptions; see for example the case of the creator of 'StealthGenie' being prosecuted by the United States Department of Justice (2014)). Furthermore, as described by Burkart and McCourt (2017: 49), "the commodity chain for hacking products and services has evaded comprehensive, or even substantial, regulation to date". A UN Special Rapporteur similarly suggested that the industry "is virtually unregulated as States have failed to keep pace with technological and political developments" (La Rue, 2013: 75). Therefore, absent meaningful regulation at the nation-state or international level, the industry has developed in a context beneficial to concealing information whilst avoiding documentation as to its practices, scale, and scope.

It is documented, however, that governments throughout the globe have purchased and deployed spyware, often in contexts of questionable legality, oversight, or minimal consideration for human rights concerns. Research by the Citizen Lab, for instance, has indicated abusive use by the Ethiopian government (Marzcak et al., 2015a) as well as the government of the UAE (Marzcak and Scott-Railton, 2016), and they strongly suspect 33 different governments of using 'FinFisher' software developed by the English-German firm 'Gamma International' (Marczak et al., 2015b). Beyond governments acting as a key consumer of spyware, Buckart and McCourt (2017) have argued that there is a "revolving door of management positions in industry and government",

with hacking software being "at least partly subsidized by the public sector" and certain developing teams receiving "de facto state support" (Buckart and McCourt, 2017: 40–41). Moreover, key governments have facilitated the industry to flourish and trade. The British government, for instance, has licensed the sale of spyware to the governments of Honduras, Saudi Arabia, Bahrain, Turkey, and Egypt, despite the recognized and credible expectation that such software could and would be used for human rights abuses (Lakhani, 2018).

An aspect of the spyware industry more relevant to this article is the push to sell spyware to general consumers. Accurate information on the number of subscribers to such services is often unforthcoming, but hacks have revealed that 'Retina-X' and 'Flexispy' have at least 130,000 general-use customers (Franceschi-Bicchierai and Cox, 2017). One of the most prominent vendors, 'MSpy', reportedly has 2 million subscribers (Cottle, 2014), but has elsewhere stated that only 27,000 Americans subscribed to their service in the first quarter of 2018 (Valentino-DeVries, 2018). Head of sales for MSpy, Andrew Lobanoff, suggests that their customer base is 40% parents monitoring their children and 15% small businesses monitoring employees (with 45% generally unknown or unaccounted for) (Cottle, 2014). It is apparent, therefore, that a concerted effort is being made to advertise and sell spyware to a wider more general-use consumer base.

Despite most jurisdictions having legal provisions such as such as Australia's Surveillance Devices Act (2004), or the Criminal Code of Canada (1985), prohibiting interception of personal communications or information without the knowledge of those involved, spyware is commercially available to mass audiences. Trade is permitted, however, on the grounds of spyware's 'legitimate' uses (Citron, 2015) that involve circumstances where both parties – the target and the operator – consent to the surveillance. Within the context of this affordance, spyware is presently available for general consumption. In Australia, for example, spyware is readily available on the internet and can be purchased directly from vendors. Additionally, software that has surveillance capabilities can be found within the popular 'Google Play Store' and 'Apple App Store'. While both stores generally restrict software that strongly self-identifies as 'spyware', they do host less intrusive versions of spyware such as 'mSpy Lite'.[1] Both stores also have policies that bar malware or deceptive applications from being sold, but powerful surveillance applications such as 'Cerberus Anti-Theft' that allow users to track devices, remotely access the camera, and receive call-log information amongst other features, can be found on the Google Play Store.[2] Furthermore, both stores also have a large range of applications with surveillance capabilities marketed as family tracker programmes, anti-theft programmes and employee trackers (Chatterjee et al., 2018).

To differentiate 'spyware' from other software with significant surveillance or data-sharing capacities, it is pertinent to establish a suitable definition. In 2005, a US Federal Trade Commission Staff Report defined spyware as "software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge" (United States Federal Trade Commission, 2005: 4). However, such a definition could arguably include a wide range of 'legitimate' platforms such as Facebook or native operating system functions. Therefore to better delineate the objects of interest considered here, for the purposes of this study we consider a programme to be 'spyware' if the following key conditions are satisfied:

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

(b) 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 permissions to disclose information.
(c) 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, as well as internet-of-things devices).
(d) 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.).

Furthermore, 'consumer spyware' is regarded as any software that satisfies the above conditions, but is sold on an open market and functions to share collected data with a specific consumer.

The risks and damage of general consumer spyware

The ease-of-access to highly intrusive surveillance software that can be deployed by non-specialist users creates a number of obvious social risks. One risk is that spyware is implicated in situations of family violence, where a developing academic literature outlines the range, scope, impact, and damage of spyware in the context of abusive intimate-partner relations (see for example Chatterjee et al., 2018; Citron, 2015; Douglas and Burdon, 2018; Eterovic-Soric et al., 2017; Freed et al., 2017, 2018; Levy, 2015). Citron (2015: 1257), for example, outlines how there have been a number of notable cases in the United States where perpetrators used spyware to track down partners, with the result of them murdering those individuals and sometimes also their children. Likewise, after consulting with a sample of 39 survivors of intimate-partner violence and 50 sector professionals, Freed et al. (2018) report that there were three confirmed cases of spyware and 47 reported instances of tracking software being used maliciously, including 10 cases where children were provided with compromised devices to track the partner (Freed et al., 2018: 4–6). In addition to the three confirmed cases of spyware, there was a much wider range of survivors and professionals who had strong suspicions and circumstantial indicators that spyware was being used, despite their inability to prove it definitively (Freed et al., 2018: 6).

The findings of Freed et al. (2018) echo statements from the family violence sector on the impact of malicious surveillance technology amongst their clients. In the UK, research by Women's Aid suggested that 29% of abuse victims experienced the "use of spyware or GPS locators" (Women's Aid, 2018), the National Stalking Helpline (UK) received 130 reported cases of spyware in 2017 (Lyons, 2018), and in Australia, surveys of domestic violence practitioners report that 74% had seen "tracking via smartphone apps" amongst their clients (Re:Charge, 2015: 6). Similarly, the National Network to End Domestic Violence (NNEDV) in the US has also stated that 72% of victim service providers had clients who were "stalked through the use of a stalking app or GPS or location tracking device" (Southworth, 2014: 3). It is clear therefore that the rise of the consumer spyware industry is creating a unique challenge for the family violence sector as its products

provide malicious actors with new opportunities and possibilities to commit abuse, harassment, and intimidation.

Spyware deployed by parents onto devices used by their children – one of the principal 'legitimate' uses of spyware marketed by the industry – can also be damaging, if not also a clear aid to child abusers. As outlined by Marx and Steeves (2010), children are increasingly bound up in surveillance apparatus as both subjects and agents of surveillance, raising a clear set of normative, cultural, and legal problems around the privacy entitlements of children and the limits of parental expectations of control over their children. A dominant frame of discussion about the necessity or acceptable scope of parental monitoring and surveillance of children includes increasing calls to reinforce children's right to privacy in the digital age, particularly in light of potentially invasive efforts to ostensibly 'protect' them using monitoring software (see for example Livingstone et al., 2015; Qvist, 2015; Shulevitz, 2013). A study by Thumala et al. (2015: 19) on electronic tracking devices, for instance, demonstrates that child-tracking still faces a "high-level of cultural and moral resistance", because parents often perceive the deployment of such surveillance as damaging to healthy relationships with children. However, in spite of spyware being couched in an ethics of care, it simultaneously could be viewed as a challenge to article 16 of the UN Convention on the Rights of the Child (Unicef, 2018) which aims to protect the privacy of children, given how it affords parents or guardians the capacity to subject children to violating and potentially abusive forms of surveillance.

Even when spyware is deployed 'legitimately' or legally, it can be corrosive and damaging to other forms of social relations and digital security. Within the context of industrial relations, for example, spyware deployed in the workplace – typically by employers on employees for the purposes of performance management – can also be coercive and intrusive. Unions within Australia are increasingly concerned about legal provisions that permit employers and insurance companies to conduct excessive surveillance (Burgess, 2018). Organizational psychology research has underlined how electronic monitoring of employees can be experienced as an unjustified invasion of privacy and can lead to perceived unfairness, decreased job satisfaction, reduced commitment, and increased work-related stress (Tomczak et al., 2018: 253–254). Furthermore, the use of spyware for employee monitoring also relies on vulnerabilities in the security and integrity of information communication infrastructures, creating weaknesses that can be exploited by additional malicious actors (ASERT, 2018).

'Spyware' is therefore what Loader et al. (2014: 469) would refer to as a "morally troubling" service. It affords operators extensive powers of surveillance that have significant capacity to cause damage to individuals and social relations, as well as to undermine broader moral and cultural norms around privacy and digital security. Whether deployed entirely 'legitimately' or illegally, spyware has the capacity, as shown, to threaten personal autonomy while fuelling corrosive relations between parents and children, intimate partners, and employees and employers, in addition to the already established and documented damage that spyware can do when leveraged against journalists, activists, political actors, and commercial operations. However, as Lyon (2007) points out, practices of surveillance often assume a logic of care which simultaneously exists as a form of control. This double-edged potential presents a fine line between what, on the one hand, might make the use of spyware appear as premised on a morally justifiable ethic of 'safety', and yet, on the other, can affirm strategies of surveillance that are ripe for controlling behaviour, manipulation, distrust, and even physical violence. In the context of this potential 'moral ambiguity' around spyware, the packaging and commodification of the software for general consumption and deployment therefore deserves closer attention.

A 'sociology of security consumption'

Goold, Loader, and Thumala (2010: 17) have called for a "sociology of security consumption" that focuses on:

> … how specific security objects are produced, promoted and received; to how these objects are (or are not) constituted as being able to secure one's person, loved ones, property, neighbourhood or interests, and to tracking the social trajectories and fate of different objects over time and through space.

They argue that critique must "analyse the ways in which competing social meanings are attached to the multitude of commodities that are produced, circulated, and consumed in a bid to make us safe and secure" (Goold et al., 2010: 6). In this spirit, it is necessary to scrutinize the commodification of spyware for a general audience. It is also appropriate to critically reflect on what this might mean for social relationships that are increasingly performed and mediated through digital modes of communication (Danaher et al., 2018).

Focusing on personal GPS tracking products, Thumala, Goold, and Loader (2015) subjected GPS trackers to an analysis from the perspective of their 'social life' that examined how meaning is intentionally manipulated by producers and how the items were received and understood by consumers. As they discovered, security products carry a social meaning that is often more important to purchasing decisions than any practical or crime control value that the device may have (Thumala et al., 2015: 6). In other words, the buying and selling of security goods clash against moral and cultural values (Loader et al., 2014). In the case of GPS trackers, the product is often viewed as too controversial from the perspective of privacy, healthy trust-relationships, and the violation of social norms to be readily embraced by consumers (Thumala et al., 2015).

This analysis was grounded in a 'close reading' of marketing materials, along with interviews and focus groups with interested stakeholders such as personnel from the tracker companies and discussions with parents (Thumala et al., 2015: 4). Following their agenda and template for a 'sociology of security consumption', we apply the same analytical lens to commercial mobile spyware. As will be shown, the chief legitimate uses of spyware are presented in terms of its provision of security and it therefore falls within the realm of a 'security product' that ought to be analyzed within a 'sociology of security consumption' that pays close critical attention to how spyware companies are engaged in selective representation of their products. Like any security product, the producers attempt to manufacture an image and context for which to interpret their commodity. The next section explains how the "narratives and social imagery that companies deploy in an effort to generate and sustain demand for protective products" (Thumala et al., 2015: 17) will be scrutinized with respect to commercial spyware.

Methods and data

An analysis of the social meaning that spyware vendors attempt to ascribe to their products requires an engagement with both the visual and textual elements of their websites and marketing materials. Such a semiological analysis probes the 'message' and 'connotations' of images and text, and the interplay between both (Barthes, 1977: 15–31). Some scholars have argued that criminology has often "neglected" the visual (Ayres and Jewkes, 2012: 315), and only recently have scholars sought to redress this analytical gap (Carrabine, 2016; Young, 2014). As argued by

Ayres and Jewkes (2012: 329), "images provide us with 'data' not necessarily available in other forms of representation", and any analysis of the meaning of consumer spyware must probe the images, in addition to the text, provided to represent the product.

While analyzing images is crucial to developing a deeper understanding of the products of the private security industry, any analysis must be attuned to the pitfalls of such semiotic analysis. As outlined by Carrabine (2016: 254), semiotic analysis has weaknesses around methodological replicability and there is also a clear risk of over-generalizing readings of particular images. Young (2014: 161) also warns of 'object-centred' analysis and provides a reminder to consider the "relation between the spectator and the image" and not ignore the meaning that is derived from the "affective nature of the spectator's encounter with the image". It should be noted, however, that this research was unable to engage with how prospective spyware clients related to the marketing images of vendors. Such a task has clear feasibility and recruitment challenges, and our attention was instead focused on how the vendors, as key actors in a sociology of consumption, depict their own products.

Any semiological analysis, therefore, has clear methodological and conceptual limitations. Interpretations, notes, or observations taken from visual materials are inseparable from the reader's prior prejudices and ideological biases, and the context from which they encounter the visual object. This is true of both scholarly researchers as well as the hypothetical web-browsing consumer of spyware. There is no definitive way to interpret the visual messages and symbols that are found within the websites of spyware vendors, but analysis of images becomes unavoidable "given the ascendant position of the image/visual in contemporary culture" (Hayward, 2010: 9, cited in Young, 2014), and because companies make a concerted effort to cultivate an interpretation of their products through imagery. Any attempt to understand the meaning given to products must therefore engage with the implied or explicit message supplied by the producer, and scholars must attempt to unpack the ideological material carried within such images and text (Ayres and Jewkes, 2012: 323).

Reflecting on this, the authors conducted a semiological analysis of nine spyware products. The sampling decision to focus on nine particular vendors followed a market analysis. The first stage of the market analysis involved doing a search of the open-web and the major app stores of Apple App Store and Google Play. Open-web searches used terms like 'spyware' and the goal was to identify prominent spyware vendors who have high search engine presence. It was assumed that the most lucrative and successful spyware vendors on the market would be those benefiting most from enhanced Google search engine optimization (SEO). Using search terms such as 'top spyware apps' also identifies a number of curated lists of spyware that collates recommendations for curious browsers (see Figure 1). There are numerous lists, including www.bestphonespy.com, www.cellspyapps.org, and www.top10spyapps.com. These lists function to draw browsers towards particular vendors and aim to be useful reviews and recommendations for potential users (see Figure 2). While these lists have sometimes been identified in the marketing material of spyware companies as part of their own self-driven advertising strategy, they have the same effect of disproportionately funnelling users to particular products and services. After using open-web searches and consulting with a number of curated lists, the research team created a 'long-list' of available spyware.

Parallel to the open-web search was a scan of the Google Play and Apple App Store. Both stores were subjected to search terms such as 'spyware', 'surveillance', 'tracking', 'spouse

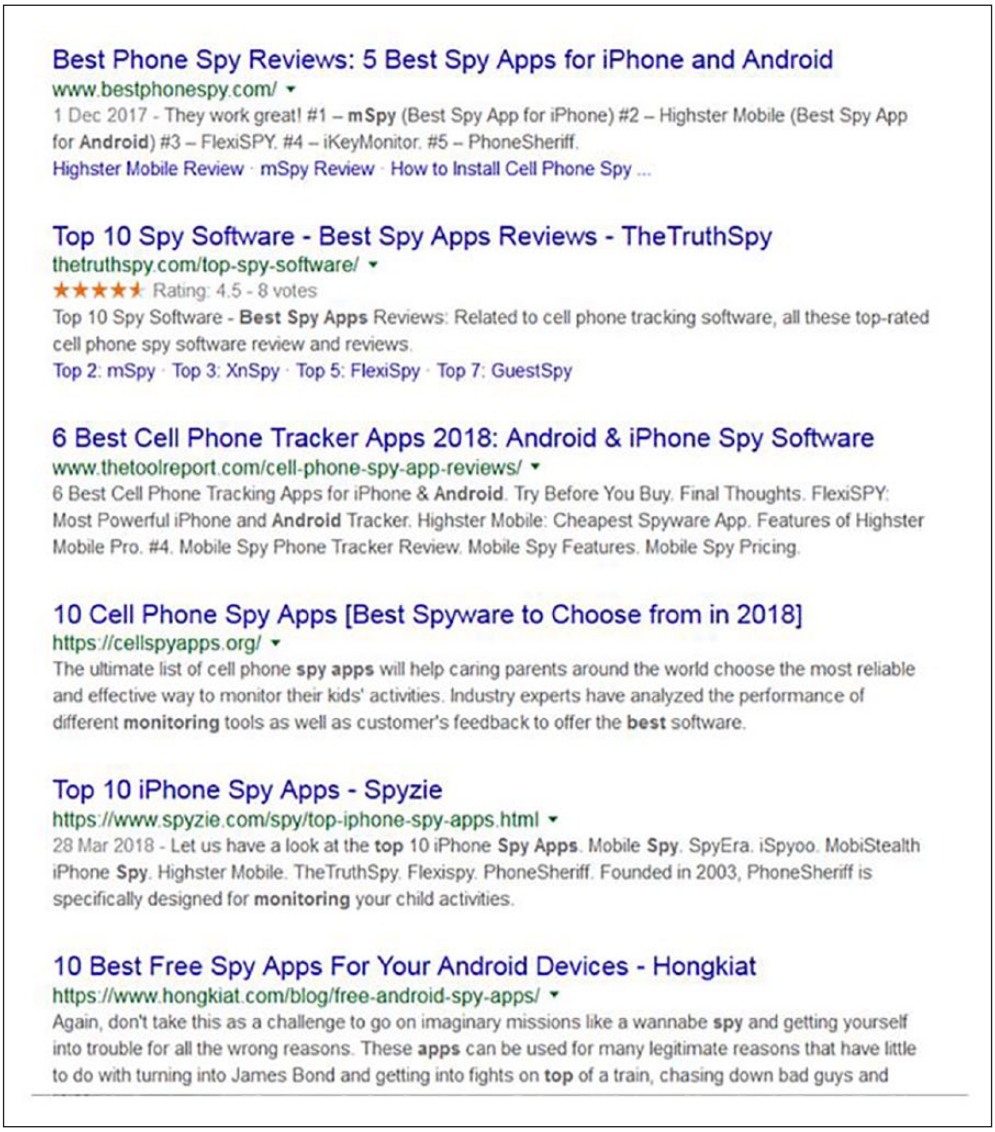

Figure 1. Showing an example of the many curated lists making recommendations on the 'best' spyware available. Search term: 'top spyware apps'. Screenshot taken on 25 April 2018.

monitoring', and 'employee tracking'. While searching for 'spyware' often produces results for 'spyware detection' software, the stores host an abundance of apps that have tracking capabilities similar to open-web spyware.[3] As described by Freed et al. (2018: 2), "in addition to apps that are frequently advertised as spyware … abusers frequently exploit *dual-use* applications – tools whose main purpose is legitimate but that can be easily repurposed to function as spyware" (emphasis in original). The Google Play and Apple App Stores contain a large number of apps that could be described as 'dual-use' which are marketed variously as trackers for family members or employees

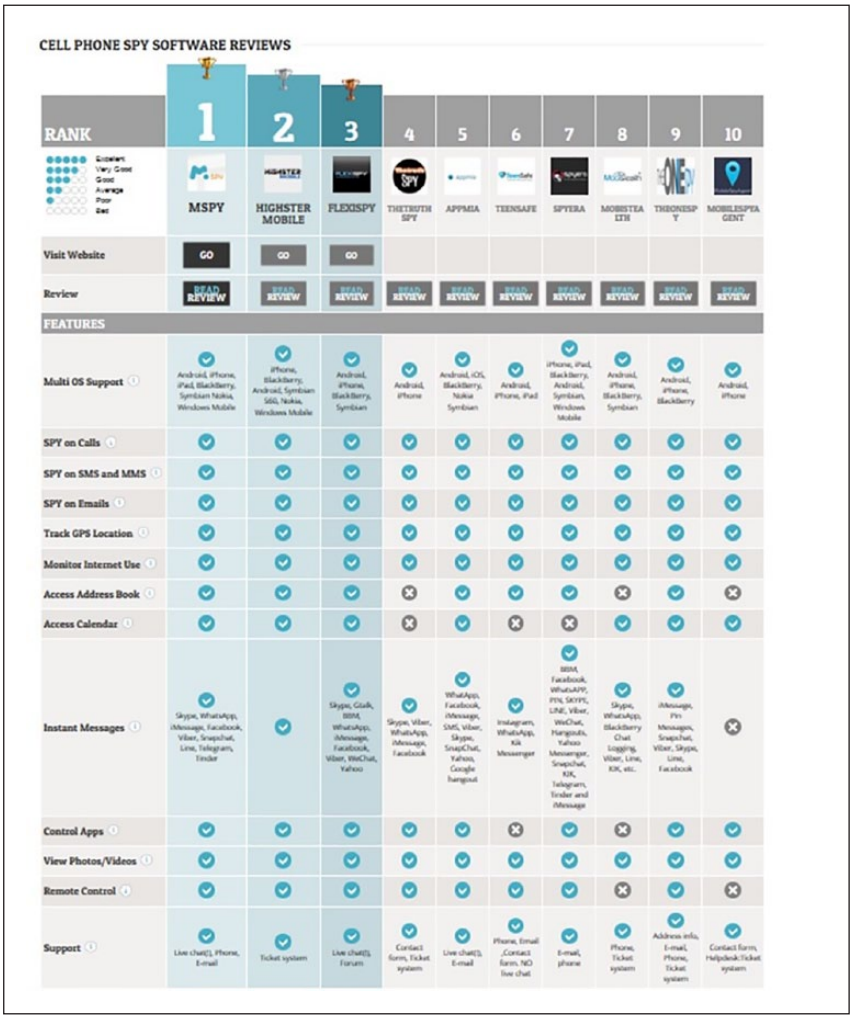

Figure 2. An example of the curated list of spyware within www.top10spysoftware.com. Note the breakdown of capabilities and ranking system for the 'best' spyware. The independence of these 'reviews' from vendors cannot be ascertained. Screenshot taken on 25 April 2018.

but can be foreseeably implemented for malicious surveillance. The research team produced a long-list of store-based apps, though it became quickly apparent that any such long-list would not exhaustively capture all of the potential 'dual-use' apps given the large number of products within the stores and the wide range of purposes under which spyware functionalities could be badged. This is further complicated by spyware often entering the app stores masquerading as more benign products, such as a messenger app (see Millman, 2017).

Based on the challenge of classifying dual use applications in the App Stores, this research chose to place more emphasis on the open-web apps. Using the long-list of apps from the open web, the team then attempted to narrow down which apps have the most prominence within

Australia. Using the 'Google Trends' feature that allows users to make comparative inquiries into topics and their frequency of being searched on Google, the research team were able to make an approximate determination of which spyware was most frequently searched for. Apps within the long-list were cross-compared and a short-list of the most prominent apps in the Australian context were determined as being:[4]

1. mSpy
2. Hoverwatch
3. Flexispy
4. TheTruthSpy
5. Highster
6. Teensafe
7. Mobistealth

Additionally, two spyware apps that feature on the Google Play store were also chosen: Cerberus and Trackview (also available in the Apple App Store).[5]

Following the selection of the nine apps, the sample was then subject to content analysis. A template was created for analyzing each website/product. Each app was subject to the same set of queries such as 'What appears when you Google [app name]?', 'What is the central marketing message of the website's front-page?', and 'What are the range of functions promised?'. Screenshots, notes, and web-links were taken in response to each query. If the app or vendor in question had a privacy policy, the policy was also subject to another set of specific questions such as 'Is there a link to the privacy policy on the homepage?', 'Is there a statement concerning which nation court proceedings must go through?', and 'Is there a description/discussion of who you can complain to if you're unsatisfied with the information/processes given by the organization?'. Once each website was processed using the content analysis template – and where relevant, the privacy policy template – a further level of comparative analysis was performed that identified the key themes of how the various spyware apps were marketed, who was depicted as the intended users of the spyware apps, in what context were the spyware apps suggested to be used, and so on. From this comparative analysis key shared themes and tropes were identified for how spyware vendors attempt to give meaning to their product.

Results

The following are the principal observations from conducting a semiotic analysis of the sample of spyware vendors:

(a) Children, employees, intimate partners and potential thieves were depicted as the suggested targets of spyware

Across the sample there was a recurring message that spyware was to be directed against four principal targets: children, employees, intimate partners, and would-be thieves. Table 1 provides an overview of whom each vendor suggested could be targeted using their software.

Spyware vendor	*Explicit suggestion to use the software to target children?*	*Explicit suggestion to use the software to target employees?*	*Explicit suggestion to use the software to target intimate partners?*	*Explicit suggestion to use the software for anti-theft purposes?*
MSpy	Yes	Yes	No	No
Hoverwatch	Yes	Yes	Yes (see Figure 5)	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".[6] It should be noted that Flexispy has been more explicit about this purpose in the past (see Cox, 2017).	No
TheTruthSpy	Yes	Yes	Yes	Yes
Highster	Yes	Yes	One reference is made to monitoring "those in relationships" on their website description depicted on the Google search results page.[7]	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, there are slight variations in emphasis between the vendors, but most strikingly, child monitoring was the most common and prominent suggested use. Major vendors such as 'MSpy' and 'Teensafe' opt to focus principally on "parental control" (see Figure 3).

The monitoring of intimate partners was also a major theme within the sample. 'TheTruthSpy' for instance lists "catch cheating spouse" as a primary "benefit" of the app and, as shown in Figure 4, clearly suggests monitoring "your lovers" and "your husband/wife" as one of its principal purposes. Hoverwatch similarly provides a recommendation to use the software to "catch a cheating spouse" and provides a detailed blogpost encouraging intimate-partner monitoring, including tips on installation (Hoverwatch, 2018a; see also Figure 5). Flexispy states in a tutorial video that you can "protect your relationships", and has previously used the phrase "catch cheating spouses" (Cox, 2017). Trackview encourages real-time tracking of "your spouse".[8] While Highster avoids mentioning monitoring partners within the main body of their website, their website description within Google search results states that it can be used to monitor "those in relationships".[7]

The other common target for spyware is employees. For example, 'Highster Mobile' promises the ability to "listen to employees' conversations when you are not in the office" (see Figure 6).

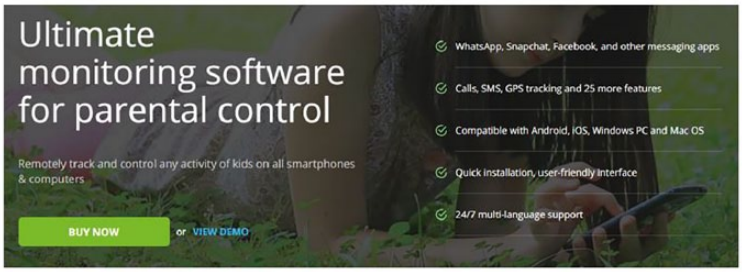

Figure 3. A depiction of the chief marketing message of 'MSpy'. Screenshot taken in February 2018.

Figure 4. Some of the suggested uses of TheTruthSpy application on their website. Note the poor grammar within "the best monitoring for protect family" (sic). Screenshot taken in February 2018.

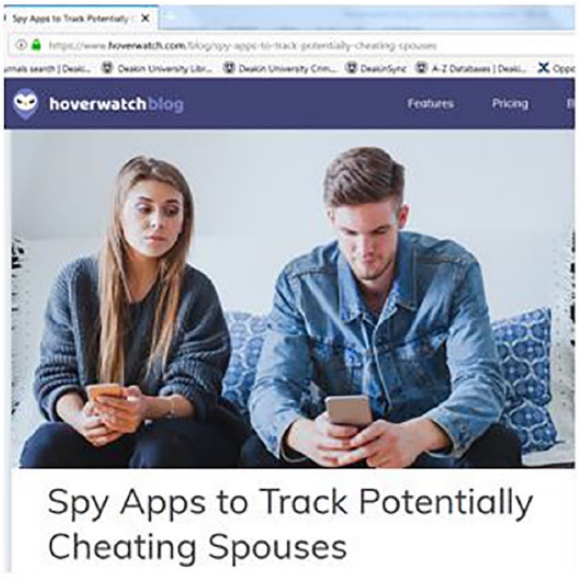

Figure 5. A blogpost from the Hoverwatch website encouraging users to target their spouses for surveillance. Screenshot taken on 31 May 2018.

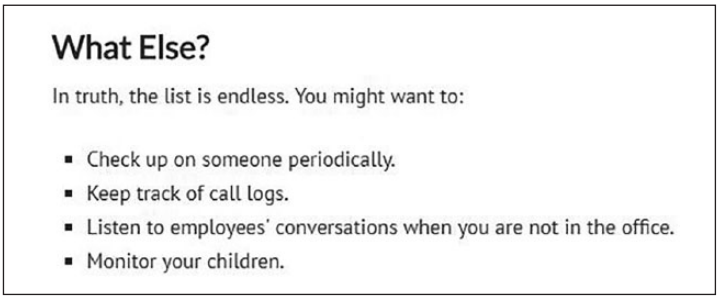

Figure 6. Some of the suggested uses of 'Highster Mobile' application on their website. Screenshot taken in February 2018.

Furthermore, spyware to be deployed as an anti-theft measure was mentioned explicitly on four occasions and is the principal marketing message behind Cerberus.

(b) The advertised level of data-monitoring is highly invasive, offering clear scope for disproportionate and abusive surveillance

Whether the software is suggested being sold to parents, employers, suspicious partners, or as an anti-theft measure, the underlying commodity was largely the same (with the exception of Trackview's more limited capabilities). Most vendors offered similar functionality in terms of capabilities and the type of data captured by the operator, regardless of the stated purpose the spyware was purported to have. Figure 2, for instance, shows a cross-comparison summary of a sample of 10 spyware apps. At a minimum, the present industry standard promises to capture phone calls, SMS messages, internet browsing, GPS location, photos, and videos, in addition to capturing the content of popular apps such as 'WhatsApp', 'Facebook', and 'Skype'. Vendors occasionally also offer subscription steps from basic to premium. 'MSpy', as shown in Figure 7, offers premium customers the added ability to block calls, block websites, snoop on the use of popular apps such as 'Tinder', and provide keylogging capability so that the operator can gain the target's confidential passwords or other text inputted on the device.

Figure 7 shows that spyware vendors offer significant surveillance capabilities to the operator (which are typically accessed by the customer through a web portal). Once an app such as 'MSpy' (premium) is deployed on someone's phone, the operator can harvest a vast amount of information that can be used for controlling, harassing, or abusive behaviour. The operator can track the movements of the target; read their intimate and personal emails, text messages, or WhatsApp communications; view their photos; activate the camera and audio-mic remotely to snoop in on conversations or private spaces; and use the keylogging service to harvest the passwords of the target which can subsequently be used to gain access to the email, social media, and perhaps financial accounts of the target, thus providing the opportunity to impersonate or 'spoof' a digital persona for malicious purposes.

(c) Vendors take steps to legitimize their product using third-party endorsements

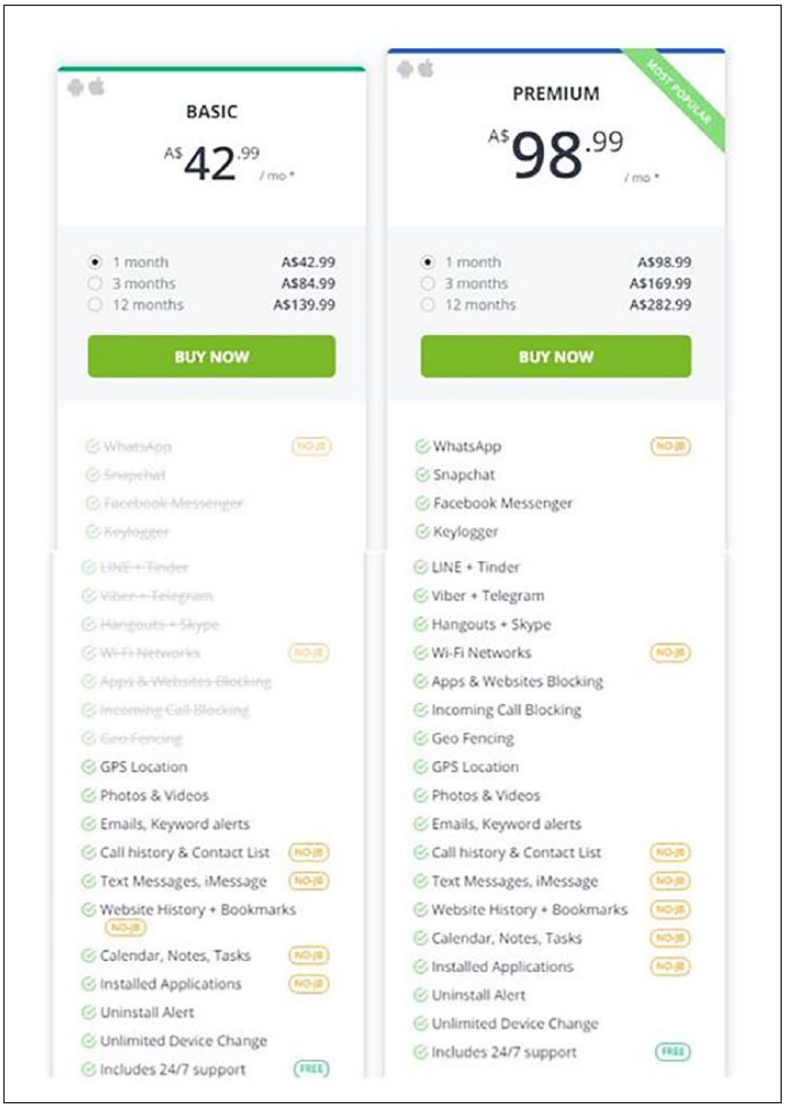

Figure 7. The advertised functionality of MSpy for 'basic' and 'premium' price brackets. Note the features which do not require the phone to be jail-broken ('NO-JB'). Screenshot taken in February 2018.

Vendors commodify and shape a 'narrative' around their product to legitimize it in spite, or because, of the potential that it might be used to facilitate inappropriate or unlawful activities, such as stalking or abuse. Customer and third-party testimonies, for instance, create the impression of spyware being used in healthy and socially productive contexts. Vendors often use a curated list of positive customer testimonies which outline how spyware provided succour to its users and solved relationship problems. Notably, comments from users such as those found in the popular App stores (which are not under the control of the vendor) – reveal how users interpreted the use of their

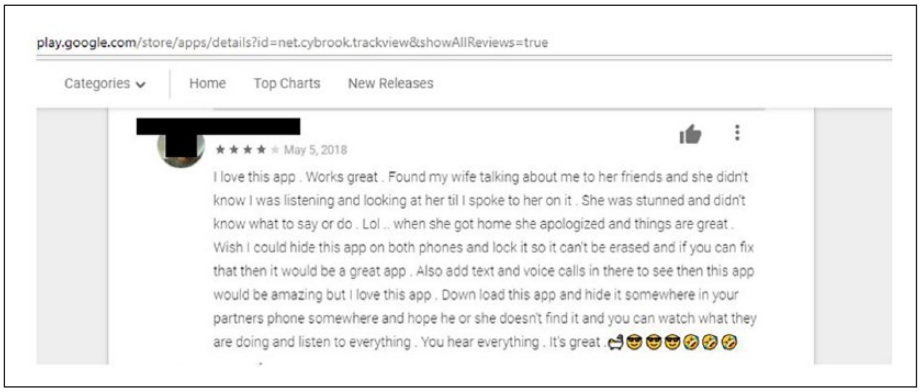

Figure 8. A user comment on Trackview within the Google Play Store. Screenshot taken on 27 May 2018.

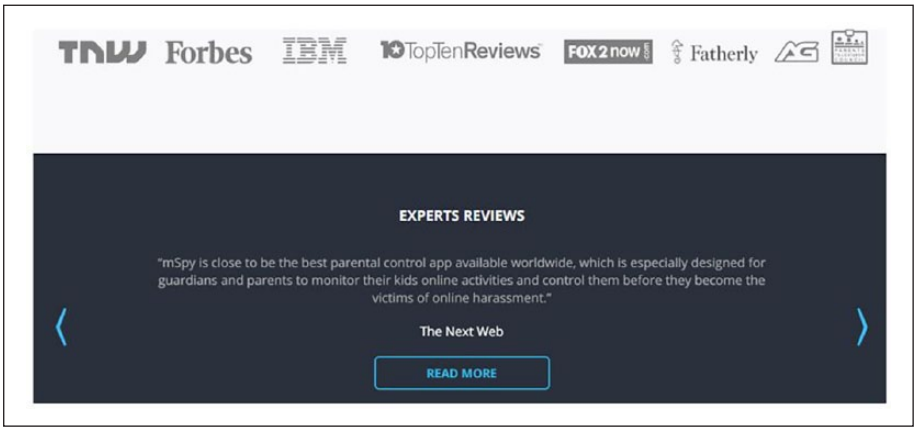

Figure 9. The use of third-party logos by 'MSpy' for advertising and legitimizing their product. Screenshot taken in February 2018.

products. For instance, see Figure 8, where a review of Trackview in the Google Play Store describes how one user encourages others to use it to spy surreptitiously on their partners.

Furthermore, a number of vendors also use the logos and symbolic authority of known brands within their website to legitimize their product. 'MSpy', for instance, uses the logos of 'Forbes' and 'IBM', amongst others (see Figure 9), while 'TeenSafe' uses specific quotes from celebrities such as Rosie O'Donnell from the popular US talk show *The View* (see Figure 10).

(d) Legal disclaimers are used to emphasize that liability for abusive use of the software rests with the user

In recognition that spyware has clear scope for being used abusively, another common element of spyware vendors' websites are the legal disclaimers and statements pertaining to the potential

Figure 10. The use of third-party logos and endorsements for 'TeenSafe' for advertising and legitimizing their product. Screenshot taken in May 2018.

> 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 11. A portion of the terms and conditions for 'Highster'. Note the absolution of 'Highster' of liability and recognition of the illegality of installing spyware without consent. Screenshot taken in February 2018.

misuse of the software. Most vendors feature an explicit or implicit acknowledgement that the product can be deployed maliciously and therefore provide a statement directing users to consider the legality of their intended use. Typically, responsibility is shifted onto the purchaser to deploy the software legally (as an example, see Figure 11 for a snippet of the terms and conditions from 'Highster'). Most vendors provide such a statement outlining that it is illegal to use the software without the consent of the target and that the responsibility rests with the user to obey local laws. As noted by Citron (2015: 1264), however, US federal law outlines that such disclaimers "do not immunize" manufacturers from potential conviction and that a vendor cannot use disclaimers for the purposes of "closing his eyes to the [surreptitious] nature and use of the devices". Furthermore, existing rulings by the US Federal Trade Commission indicate that spyware poses legal challenges regarding consumer protections (see e.g. McKune and Deibert, 2017: 17–19; US Federal Trade Commission v. CyberSpy Software, 2010). Regardless of the protections afforded by such disclaimers, it is a notable feature in the marketing of spyware that vendors recognize the potential for misuse of their product and attempt to avoid any potential liability.

(e) Claims within legal disclaimers often clash with other content on the website that suggests or encourages non-consensual use

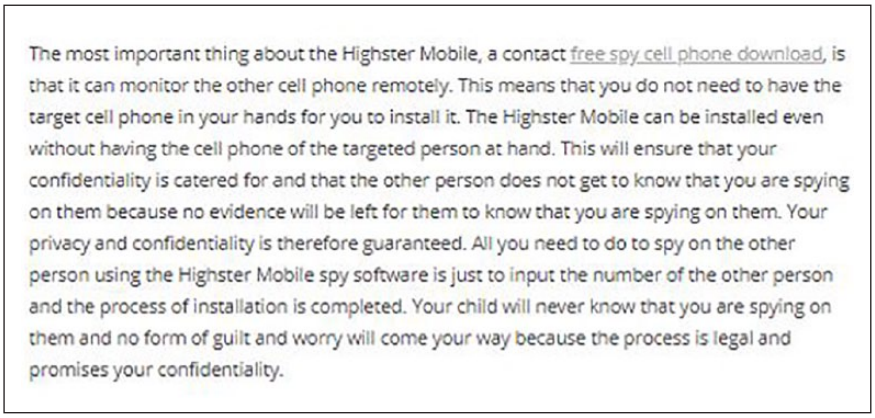
The most important thing about the Highster Mobile, a contact free spy cell phone download, is that it can monitor the other cell phone remotely. This means that you do not need to have the target cell phone in your hands for you to install it. The Highster Mobile can be installed even without having 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 12. An excerpt from a blog on the 'Highster' website: https://highstermobile.com/blog/category/highster-mobile-app/ (accessed and screenshot taken in February 2018). Note the emphasis on supporting entirely secretive, non-consensual installation.

For several of the vendors we analyzed there is a semiotic clash between the content of their disclaimers and other prominent marketing claims made elsewhere on their website. As noted in Figure 11, 'Highster' advises against non-consensual installation of the software. Elsewhere on their website, however, 'Highster' makes claims that it can support non-consensual, unilateral, and surreptitious installation (see Figure 12) while also stating that "it is difficult to get caught while using this software" (Highster, 2019).

Examples of conflicting or contradicting messages between the content of disclaimers and marketing claims are numerous. As shown in Figure 4, for instance, 'TheTruthSpy' promises that its app is "100% undetectable", whereas in its terms of use it is stated that "it is forbidden to use it for purposes described as devious, unbeknownst to the person using the phone" (TheTruthSpy, 2019). In this respect, prominent marketing claims encourage secretive use, while disclaimers aim to suggest consensual use only. Similarly, Mobistealth offers FAQs on how you can ensure that targets using Android will not be capable of detecting that the software has been introduced to their phone, belying the content of their end-user license agreement which states that "installing Mobistealth on another person's Phone/Computer without their knowledge can be considered as an illegal activity" (Mobistealth, 2019). Furthermore, MSpy's YouTube channel contains a video that instructs users how to install the app on Android devices with the icon hidden from the perspective of the target (MSpy, 2018a), while a blogpost on Hoverwatch encourages using the "stealth mode" to "stay hidden" in the context of spying on a partner (Hoverwatch, 2018a). Both recommendations contradict messages from their end-user license agreements that emphasize the need for "explicit permission" (Hoverwatch, 2018b) and the "consent of the device owner" (MSpy, 2018b) before installing the software.

In this respect, semiotic analysis of the websites of spyware vendors reveals a number of contradictory messages. First, it illustrates that via the legal disclaimers and terms of use statements, vendors concede and acknowledge that certain uses of spyware may be legally contentious. Second, it shows that vendors make efforts in the 'small-print' to deny liability for such malicious use and attempt to define the use of spyware only in contexts where both parties consent. This,

Figure 13. A snapshot of Flexispy's functionalities as advertised on their website. Note the ability to 'spoof SMS', which reflects an impersonation function. Screenshot taken on 2 October 2018.

however, is often contradicted within other prominent claims which refer to secretive, 'undetectable', or hidden installation that allows an operator the opportunity to anonymously, non-consensually, and unilaterally place spyware on a target's device.

(f) Certain spyware vendors offer 'spoof' SMS message functions contradicting their purported 'monitoring' function

In contradiction to its purported 'monitoring' function, 'Flexispy' also offers the capacity to send 'spoofed' messages from the phone (see Figure 13). As outlined above, the principle marketing messages suggest that the software is for a care-focused application for 'watching over' a child, employee, or intimate partner. Likewise, in its terms and conditions, it is outlined that the software is to be used as an aid for monitoring: "You acknowledge that you will only install the software on a device which you have a legitimate need to monitor, and have a legal right to do so" (Flexispy, 2018). However, the ability to send 'spoof' SMS messages from a captured device is more akin to masquerading as the target and cannot reasonably be regarded as a 'monitoring' function. It involves taking a pro-active role to remotely send messages from the device that will appear to subsequent recipients as coming from the target. Put differently, it involves assuming the identity of the target and performing actions under that assumed identity. The target has no record of the message leaving their device (the researchers confirmed that the spoof SMS function performs in this manner during subsequent technical analysis). The ability to 'impersonate' the target is not featured in the prominent marketing claims of Flexispy, nor is there any explicit mention of any potential legal ramifications in the terms of service for operators using this functionality.

(g) The 'meta-voice' of the vendors tends to address the operator (and not the target or unsuspecting third parties)

Another aspect of our semiotic analysis was to probe the websites, terms of use, and privacy policies of spyware vendors for any explicit mention or provision of support mechanisms for targets who may have been maliciously subjected to their software. It is possible that individuals could be victimized through the software, targeted without their consent, and have their data collected by the software (and most likely stored on the servers of the spyware vendor). In such circumstances there ought to be options to reclaim the data or receive clarity around which data was unknowingly extracted from the target. While the vendors provided either an email address or online form to use in the event of a complaint or a request for support for operators, there were no explicit instructions or guidance provided within our sample for targets who have been subject to their software. Language was primarily directed to customers (i.e. operators), and no clear provisions or response processes were outlined from the perspective of victimized targets.

In this regard, the 'meta-voice' of the spyware vendor's external-facing materials spoke exclusively to potential operators or users. Options, mechanisms, or potential forms of support for victims were not present. This lack of 'voice' towards potential victims demonstrates that despite claims made within disclaimers emphasizing that spyware should be deployed consensually and agreed by both parties, the vendors are currently positioned to only highlight and service the needs and interests of operators, which, as shown, are often promised 'undetectable' or 'hidden' use. No clear steps are put in place to support those abused by the software, which as the legal disclaimers acknowledge is a reasonably foreseeable outcome of selling spyware. Semiotic analysis, therefore, demonstrates the imbalanced servicing of the needs of the operator over the target, despite suggestions elsewhere that spyware should only be deployed in a context where both parties are willing participants.

Furthermore, third parties are also neglected and not mentioned within the 'meta-voice' of the vendor's websites, policies, or marketing materials. Most of the software promises to intercept SMS messages, emails, WhatsApp communications, Skype calls, and activity on apps such as Tinder. It is likely, therefore, that private communications and information from unknowing third parties will be caught in the software's dragnet. Even under the circumstances where an operator and target consent to deploying the spyware, third parties who interact with the captured device via SMS, email, WhatsApp, and so on will also see their data captured by the operator. In this respect, anyone who interacts with the captured device will see their data which is shared with the target device compromised and passed into the hands of the operator and the vendor's servers without their consent. While the legal disclaimers and end-user license agreements speak to the need for two-party consent, they neglect to recognize that third-party data will inevitably be swept up by the software's dragnet and that there is a clear duty of care to such parties. Semiotic analysis reveals, however, that the vendors speak primarily to the interests of the operator and not to the target, nor any unsuspecting third parties.

Discussion

A semiotic analysis of the consumer spyware industry reveals that there is an attempt to commodify powerful surveillance software grounded in the perspective that children, intimate partners, and employees are legitimate targets for close observation and control. Overall, justifications

of the use of spyware serve to valorize the desires of those seeking to engage in the use of spyware, while rendering less visible the ancillary impacts for digital security, privacy, and the social experiences of those that are monitored as surveillance objects. As our analysis has demonstrated, vendors primarily align themselves with the interests of user-operators and typically provide little indication of their responsibility to support the target or third parties (particularly in the event of abuse), and thus reinforce Torin Monahan's (2011: 497) perspective that surveillance most often "validates the intentions of surveillance subjects, while subordinating the experiences and agency of those monitored as objects".

Furthermore, a number of vendors also present contradictory messages to potential users, which may involve marketing claims around the un-detectability of the software and assurances that the product can be deployed surreptitiously, while 'small print' legal disclaimers aim to emphasize that only two-party consensual use is legally permissible. Furthermore, the marketing of spyware tends to emphasize the extent and scope of data that is scooped up in the software's dragnet, with no articulation that legitimate two-party consensual use might not require such expansive surveillance to serve the legitimate functions of providing ample protection to children or reasonable employee monitoring. Optional forms of limited or 'proportionate' surveillance are only occasionally offered; otherwise the marketing priorities appear to strive towards demonstrating the escalating and increasingly invasive capabilities of the software, irrespective of and untethered to a discussion of how specific data capture may relate to serving 'legitimate' uses.

Our analysis also serves the wider agenda of a 'sociology of security consumption' (Goold et al., 2010), and underlines the importance of tracking new security products and how they are commodified for consumption. Providing such an analysis highlights the often concerning practices of an industry that sells products with significant abusive potential and evident social risks. Scholars of security consumption and the private security industry alike ought to increasingly pay attention to the developing commodification of forms of software that can be deployed abusively but are often packaged and sold as a security product using a message of 'care' and 'safety'. Most research on spyware, for instance, has been largely dominated by the perspective of computer science and there are only limited examples of social scientific critique. Faizal Ab Razak et al. (2016: 63), for example, attempted to catalogue the scholarly field of study on malware and illustrated that approximately 2.6% of publications are from the humanities and social sciences, demonstrating the imbalance of focus provided by non-STEM perspectives on digital-related social problems. In this respect, a fuller 'sociology of security consumption' and more complete study of the private security industry needs to be cognizant of emerging digital markets for inherently controversial security products and play an increased role in scholarship around spyware. The results of this study also serve a wider normative purpose of highlighting the concerning commodification of software that carries significant social risks for a number of specific groups including victims of domestic violence, children, workers, and businesses, in addition to human rights activists, journalists, and other corporate or political actors. It is necessary for further research to understand and contextualize the proliferation of spyware with respect to cultural and social trends around how parents, employees, or abusive partners may justify surveilling their targets. Unpacking how specific consumer groups engage with spyware products is a key absence in the 'sociology of security consumption' presented here, and future research would deepen our understanding of spyware and strengthen our preparedness to counter its most corrosive impacts.

Overall, developments within the spyware industry and attempts to commodify surveillance software for general consumption deserve further social, political, and legal scrutiny. As outlined by

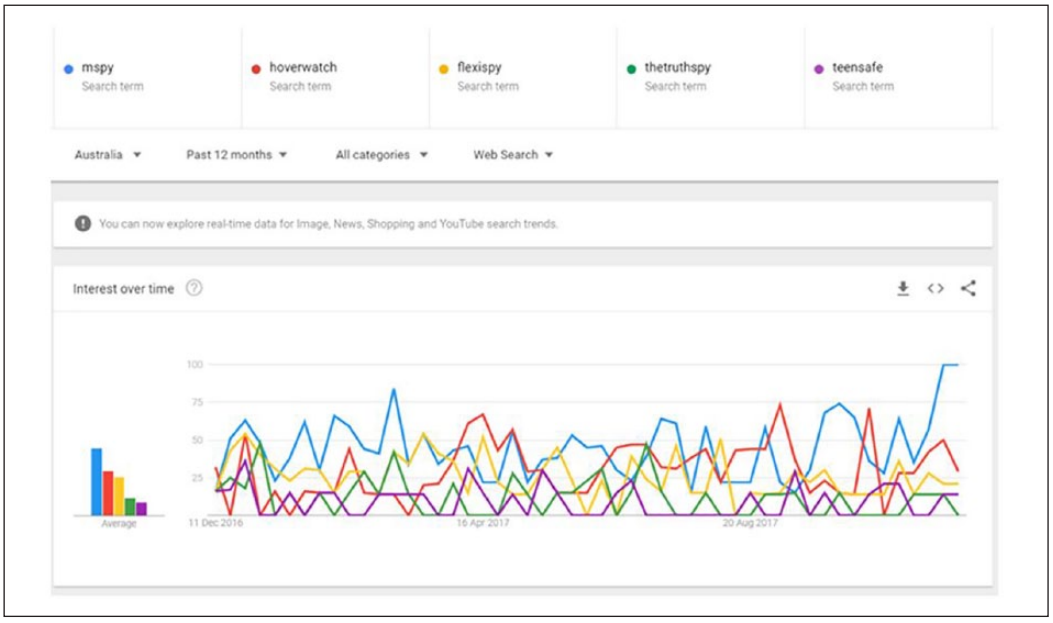

Figure 14. Screenshot showing comparison of apps on Google trends within Australia, taken 5 December 2017.

Citron (2015), in the context of the United States where there are existing laws restricting the manufacture, sale, and advertisement of spyware, in addition to laws restricting its use, such laws are often too weak and under-enforced, and in general very few regulatory or law enforcement agencies take a sufficient interest in the social problems created by such products. While spyware gains ample attention in the world of information security, and increasingly in the world of family violence advocacy groups, its "social life" (Thumala et al., 2015: 3) is still largely in the category of a "novel good" (Goold et al., 2010: 20). It is still yet to gain a widespread profile in terms of understanding, consumption, or suitable politicization as a significant problem. In this respect, the industry continues to benefit from remaining a largely concealed trade which primarily serves the interests of those who would aim to exploit the software for malicious ends as opposed to the interests of those who aim to create integrity around digital devices within a culture of healthy personal privacy and autonomy.

Conclusion

This article subjected a sample of nine spyware apps to a semiotic analysis that aimed to analyze how powerful surveillance software is commodified for a general consumer audience. Despite the underlying data-capture capabilities often being similar, different vendors chose to emphasize and create different social meanings for their product. All of the vendors analyzed, however, had to reckon with the documented association of spyware with abuse and illegal behaviour. Legal disclaimers and terms of use often underlined that the product ought to be used in a consensual context, but this was at times undermined or contradicted by other marketing content that outlined the potential for surreptitious and unilateral use. Applying this type of 'sociology of security

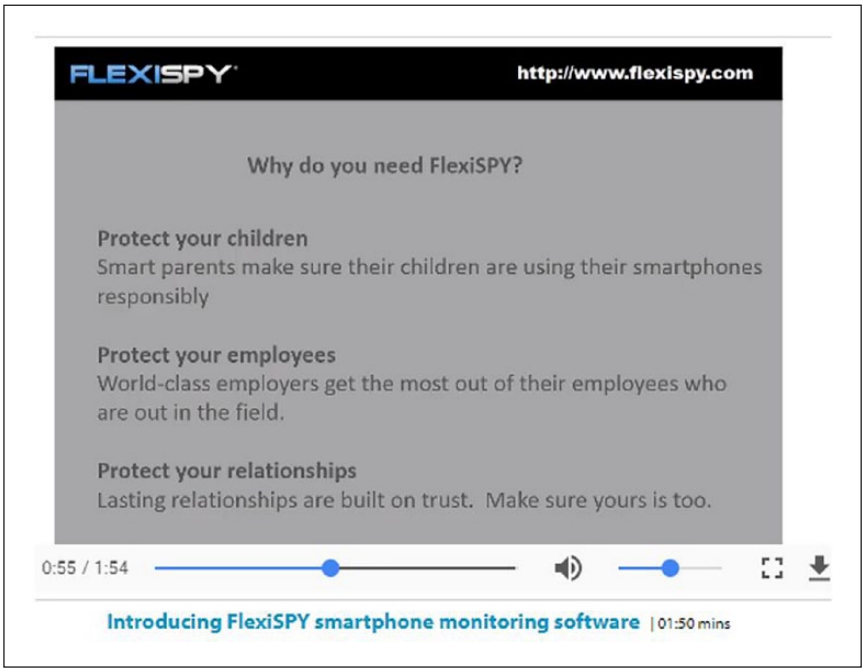

Figure 15. Screenshot from the Flexispy website, showing content from their video tutorial suggesting it is to be used targeting "your relationships".

Figure 16. Screenshot showing the website description for Highster, outlining that it can be used by those in relationships. (Screenshot taken on 2 July 2018).

Figure 17. Screenshot showing the website of Trackview, referring to the ability to track "your spouse". (Screenshot taken on 15 June 2018).

consumption' (Goold et al., 2010) to consumer spyware helps reveal the connections and contradictions between the marketing materials, the significant surveillance power of the software, the foreseeable incidents of abusive use, and the back-end attempts to indemnify developers against illegal use of their products. It also underlines and highlights the broader concerning trajectory of powerful tools of surveillance being made available and sold to a general consumer audience through using ethics of 'care' and logics of 'security' to commodify malware.

Acknowledgement
We are grateful for constructive feedback provided by Christopher Parsons, Lex Gill, Cynthia Khoo, and Miles Kenyon. Any errors or omissions are our own. Adam Molnar would also thank the Citizen Lab, Munk School of Global Affairs and Public Policy, at the University of Toronto, where he was Visiting Professor during the production of this article.

Declaration of conflicting interests
The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This research was supported and funded by a grant from the Australian Communications Consumer Action Network (ACCAN).

ORCID iD
Diarmaid Harkin https://orcid.org/0000-0002-9928-719X

Notes
1. mSpy Lite was available on Apple App Store (UK) and Google Play Store when checked on 30 April 2018.
2. Cerberus Anti-Theft was available on Google Play Store when checked on 30 April 2018.
3. For example, an app called 'PhoneWatcher – Mobile Tracker' by developers 'Lutrecamu and Tolencamut' states: "PhoneWatcher is a powerful tracking app equipped with a strong set of features that allow users to keep a check on the cell phone activities of their kids other family members or employees in order to avoid any unwanted behavior or for safety purposes. THE APPLICATION ALLOWS YOU TO: • SMS Tracking The built in SMS tracker lets you read all SMS messages sent or received. Even if the message is deleted from your child's phone, you can still read it as a copy is sent to your control panel. As well as reading the text message itself, you will also be able to see who it is from/to and when it was sent. • Monitor Cell Phone Call Logs This amazing tracking app allows you to look at call logs for both incoming and outgoing calls. You can see who your child has been calling, the time and date of the call, the duration of the calls and how many times your child makes calls to that number. • GPS Location Monitoring If you have concerns about where your child is going when they leave the house, then you are going to love the GPS tracker that is included with this phone monitoring app. You can see their movements in real time or check out a historical map showing where they have been. Not only does this let you know where they are hanging out, but in the event that your child ever went missing it could help to locate them very quickly. • Access to Complete Browsing History The internet can be a scary place at times! While it is fantastic for finding information and communicating with others, we all know it has

a darker side too. The browser history feature of Cell Phone Tracker allows you to see which sites your child is browsing. • Photo & Video Interception Cell Phone Tracker intercepts every single photo or video that is taken using your child's cell phone. This allows you to see if your child is making inappropriate images. There is a worrying trend among teens right now for 'sexting' which involves sharing risqué images with each other. This app lets you make sure that this is not happening with your child. Note: this software must be installed only by phone owner or at their consent! (GooglePlay store content logged on 4 January 2018).

4. Screenshot showing comparison of apps on Google trends within Australia, taken 5 December 2017 (see figure 14).
5. TrackView is marketed as a mobile security system that can enable users to monitor their own home, as well as locate family members and objects. In comparison to the rest of the apps in the sample, TrackView's surveillance capabilities are not as powerful. However, the app's ability to GPS track family members using mobile phones means that it can foreseeably function as malware. In addition, the experience of users, as self-reported in Google Play Store reviews, highlights that some consumers have deployed the software for the non-consensual surveillance of intimate partners (see figure 8).
6. Screenshot from the Flexispy website, showing content from their video tutorial suggesting it is to be used targeting "your relationships" (see figure 15).
7. Screenshot showing the website description for Highster, outlining that it can be used by those in relationships. (Screenshot taken on 2 July 2018) (see figure 16).
8. Screenshot showing the website of Trackview, referring to the ability to track "your spouse". (Screenshot taken on 15 June 2018) (see figure 17).

References

Armageddon E (2017) When technology takes hostages: The rise of 'stalkerware'. *Vice: Motherboard*. Available at: https://motherboard.vice.com/en_us/article/nejmnz/when-technology-takes-hostages-the-rise-of-stalkerware (accessed 22 May 2018).

ASERT (2018) *Lojack Becomes a Double-Agent*. Available at: https://asert.arbornetworks.com/lojack-becomes-a-double-agent/ (accessed 6 July 2018).

Ayres T and Jewkes Y (2012) The haunting spectacle of crystal meth: A media-created mythology? *Crime Media Culture* 8(3): 315–332.

Barthes R (1977) *Image, Music, Text*. London: Fontana Press.

Burgess K (2018) Out-of-hours worker surveillance laws to be pared back after privacy concerns. *Canberra Times*. Available at: http://www.canberratimes.com.au/act-news/outofhours-worker-surveillance-laws-to-be-pared-back-after-privacy-concerns-20180212-h0vy9k.html (accessed 30 May 2018).

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.

Carrabine E (2016) Picture this: Criminology, image and narrative. *Crime Media and Culture* 12(2): 253–270.

Chatterjee R, Doerfler P, Orgad H et al. (2018) The spyware used in intimate partner violence. *IEEE Symposium on Security and Privacy*. Available at: https://www.ipvtechresearch.org/pubs/spyware.pdf (accessed 22 May 2018).

Citizen Lab (2015) *Research on Hacking Team and FinFisher Highlighted in Motherboard*. Available at: https://citizenlab.ca/2015/11/research-on-hacking-team-and-finfisher-highlighted-in-motherboard/ (accessed 26 June 2018).

Citron DK (2015) Spying Inc. *Washington and Lee Law Review* 72(3): 1243–1282.

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

Cox J (2017) I tracked myself with $170 smartphone spyware that anyone can buy. *Vice: Motherboard*. Available at: https://motherboard.vice.com/en_us/article/aeyea8/i-tracked-myself-with-dollar170-smartphone-spyware-that-anyone-can-buy (accessed 26 April 2018).

Danaher J, Nyholm S and Earp BD (2018) The quantified relationship. *The American Journal of Bioethics* 18(2): 3–19.

Douglas H and Burdon M (2018) Legal responses to non-consensual smartphone recordings in the context of domestic and family violence. *University of New South Wales Law Journal* 41(1): 1–29.

Eterovic-Soric B, Choo KKR, Ashman H et al. (2017) Stalking the stalkers – detecting and deterring stalking behaviours using technology: A review. *Computers and Security* 70: 278–289.

Flexispy (2018) Terms and conditions of purpose. Available at: https://www.flexispy.com/en/term-conditions.htm (accessed 2 October 2018).

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

Freed D, Palmer J, Minchala D et al. (2017) Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders. *Proceedings of the ACM on Human-Computer Interaction: Volume 1 Issue CSCW*. Available at: https://www.ipvtechresearch.org/pubs/a046-freed.pdf (accessed 22 May 2018).

Freed D, Palmer J, Minchala D et al. (2018) 'A stalker's paradise': How intimate partner abusers exploit technology. *ACM Conference on Human Factors in Computing Systems*. Available at: https://www.ipvtechresearch.org/pubs/stalkers-paradise-intimate.pdf (accessed 22 May 2018).

Goold B, Loader I and Thumala A (2010) Consuming security? Tools for a sociology of security consumption. *Theoretical Criminology* 14(1): 3–30.

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

Highster (2019) Announcement: Highster Mobile Review 2019 - How Good is This Phone Spy App? Available at: https://www.highsterspyapp.com/highster-mobile/ (accessed 3 January 2019).

Hoverwatch (2018a) Spy apps to track potentially cheating spouses. Available at: https://www.hoverwatch.com/blog/spy-apps-to-track-potentially-cheating-spouses (accessed 31 May 2018).

Hoverwatch (2018b) Terms of service. Available at: https://www.hoverwatch.com/terms-of-service (accessed 3 July 2018).

La Rue F (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 at: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (accessed 22 May 2018).

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

Levy K (2015) Intimate surveillance. *Idaho Law Review* 51: 679–693.

Livingstone S, Carr J and Bryne J (2015) One in three: Internet governance and children's rights. *Global Commission on Internet Governance*. Available at: https://www.cigionline.org/sites/default/files/no22_2.pdf (accessed 22 May 2018).

Loader I, Goold D and Thumala A (2014) The moral economy of security. *Theoretical Criminology* 18(4): 469–488.

Lyon D (2007) *Surveillance Studies: An Overview*. Cambridge: Polity Press.

Lyons K (2018) Stalkers using bugging devices and spyware to monitor victims. *The Guardian*. Available at: https://www.theguardian.com/uk-news/2018/feb/13/stalkers-using-bugging-devices-and-spyware-to-monitor-victims (accessed 1 May 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 at: https://citizenlab.ca/wp-content/uploads/2017/03/citizenlab_whos-watching-little-brother.pdf (accessed 22 May 2018).

Marx GT and Steeves V (2010) From the beginning: Children as subject and agents of surveillance. *Surveillance and Society* 7(3/4): 192–230.

Marzcak 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 at: https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/ (accessed 26 April 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 at: https://citizenlab.ca/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/ (accessed 26 April 2018).

Marczak B, Scott-Railton J, Senft A et al. (2015b) Pay no attention to the server behind the proxy mapping FinFisher's continuing proliferation. *The Citizen Lab*. Available at: https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/ (accessed 26 April 2018).

Millman R (2017) Spyware found in more than 1,000 apps in Google Play Store. *SC Media*. Available at: https://www.scmagazineuk.com/spyware-found-in-more-than-1000-apps-in-google-play-store/article/681506/ (accessed 22 May 2018).

Mobistealth (2019) *End User License Agreement*. Available at: https://www.mobistealth.com/eula.php (accessed 3 January 2019).

Monahan T (2011) Surveillance as cultural practice. *Sociological Quarterly* 52: 495–508.

MSpy (2018a) *mSpy Installation Guide – Android*. Available at: https://www.youtube.com/watch?v=vJKlewQrW_c (accessed 3 June 2018).

MSpy (2018b) Terms of use. Available at: https://www.mspy.com/terms-of-use.html (accessed 1 February 2018).

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

Qvist B (2015) Parents, is it OK to spy on your child's online search history? *The Guardian*. Available at: https://www.theguardian.com/sustainable-business/2015/nov/05/parents-children-online-search-history-microsoft-windows-10-privacy (accessed 1 May 2018).

Razak MFA, Anuar NB, Salleh R et al. (2016) The rise of 'malware': Bibliometric analysis of malware study. *Journal of Network and Computer Applications* 75: 58–76.

Re:Charge (2015) ReCharge: Women's technology safety, legal resources, research and training – National study findings 2015. Available at: http://www.smartsafe.org.au/sites/default/files/ReCharge-Womens-Technology-Safety-Report-2015.pdf (accessed 1 May 2018).

Shulevitz J (2013) Big mother is watching you. *The New Republic*. Available at: https://newrepublic.com/article/115347/parental-surveillance-creepy-new-ways-spy-your-kids (accessed 1 May 2018).

Southworth C (2014) The testimony of the National Network to End Domestic Violence with the Minnesota Coalition for Battered Women. Hearing of the Senate Judiciary Committee Subcommittee on Privacy, Technology and the Law. 4 June. Available at: https://www.judiciary.senate.gov/imo/media/doc/06-04-14SouthworthTestimony.pdf (accessed 22 May 2018).

The Truth Spy (2019) *Terms of Use/Legal*. Available at: http://thetruthspy.com/terms-of-use/ (accessed 3 January 2019)

Thumala A, Goold B and Loader I (2015) Tracking devices: On the reception of a novel security good. *Criminology and Criminal Justice* 15(1): 3–22

Tomczak D, Lanzo L and Aguinis H (2018) Evidence-based recommendations for employee performance monitoring. *Business Horizons* 61: 251–259.

Unicef (2018) UN Convention on the Rights of the Child. Available at: https://www.unicef.org.uk/what-we-do/un-convention-child-rights/ (accessed 1 May 2018).

United States Department of Justice (2014) Man pleads guilty for selling "StealthGenie" spyware app and ordered to pay $500,000 fine. Available at: https://www.justice.gov/opa/pr/man-pleads-guilty-selling-stealthgenie-spyware-app-and-ordered-pay-500000-fine (accessed 26 April 2018).

United States Federal Trade Commission (2005) *Spyware workshop: Monitoring software on your personal computer: Spyware, Adware and other software report*. Available at: https://www.ftc.gov/sites/default/files/documents/reports/spyware-workshop-monitoring-software-your-personal-computer-spyware-adware-and-other-software-report/050307spywarerpt.pdf (accessed 26 June 2018).

United States Federal Trade Commission v. CyberSpy Software, LLC, et al., No. 08-CV-01872 (M.D. Fla. Apr. 22, 2010), (stipulated final order). Available at: https://www.ftc.gov/sites/default/files/documents/cases/2010/06/100602cyberspystip.pdf

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

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

Young A (2014) From object to encounter: Aesthetic politics and visual criminology. *Theoretical Criminology* 18(2): 159–175.

Author biographies

Diarmaid Harkin is a senior lecturer in Criminology at Deakin University. He is currently an Alfred Deakin Postdoctoral Research Fellow based at the Alfred Deakin Institute for Citizenship and Globalisation. His current active research projects examine the consumer spyware industry, cyber-policing, and the use of private security companies by family violence services in Australia.

Adam Molnar is a lecturer in Criminology at Deakin University where he is a member of the Alfred Deakin Institute for Citizenship and Globalisation. Molnar completed a postdoctoral fellowship at the Queen's University Surveillance Studies Centre (Canada), a PhD at the University of Victoria (Canada), and is currently a Visiting Professor at the Citizen Lab in the Munk School of Global Affairs and Public Policy at the University of Toronto. Much of his work focuses on the intersection of technology and socio-legal studies with a particular focus on surveillance and privacy in Australia and Canada.

Erica Vowles is a journalist and broadcaster with the Australian Broadcasting Corporation. Much of her journalism focuses on social policy and legal issues. Erica also conducts independent academic research. Erica completed a BA of Arts at Charles Sturt University and a Masters in International Relations at the University of NSW.