Stalking the stalkers – detecting and deterring stalking behaviours using technology: A review

Brett Eterovic-Soric, Kim-Kwang Raymond Choo, Helen Ashman, Sameera Mubarak

School of Information Technology & Mathematical Sciences, University of South Australia, Adelaide, SA 5001, Australia
Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249-0631, USA

ABSTRACT

The Internet age has brought with it a slew of tools and research which allow stalkers, from ex-lovers to complete strangers, to follow a person’s life in great detail without their consent. The converse side of the issue, the ability of a target to detect and track stalking behaviour, has not received nearly as much attention, with privacy and security research largely discussing other threat models. This article reviews the current literature on the subject and explores the disparity between technologies used by stalkers and technologies used against stalkers, then suggests some research avenues which may help correct this imbalance.

© 2017 Elsevier Ltd. All rights reserved.

Keywords: Cyberstalking Cyberstalker Online surveillance Counter-surveillance Privacy Spyware

1. Introduction

William Shakespeare is said to have described the thought process of a stalker in his later sonnets (Skoler, 2001). Sting sung about obsessively watching the object of his affection in The Police’s 1983 hit single “Every Breath You Take”. Overwhelming persistence during the courting process is depicted as a virtue in films such as Love Actually.

In reality, persistent unwanted following is often more traumatic than romantic. Famous cases involve the stalking of celebrities such as Madonna and David Letterman, but the majority of stalking cases concern two (or more) ordinary people who were lovers or acquaintances. Prior to the 1990s this behaviour was not illegal, and unless a stalker broke some other law by trespassing or committing assault, police had very few options for helping the victim. In 1989, Robert Bardo shot the actress Rebecca Shaeffer on her doorstep, after having researched and followed her for two years (de Becker, 1997). This incident and the resulting media attention led to the development of the first anti-stalking laws, in California (Perez, 1992, p. 269).

* Corresponding author.
E-mail address: raymond.choo@fulbrightmail.org (K.-K.R. Choo).
http://dx.doi.org/10.1016/j.cose.2017.06.008
0167-4048/© 2017 Elsevier Ltd. All rights reserved.
Stalking is a pattern of behaviour with many definitions. The legal definitions differ from country to country and from state to state, influenced by local stalking cases as the laws were being enacted (similar to other cyber-related offences, such as online child exploitation - Hillman et al., 2014). However, they are characterised by the persistent unwanted following of a person, causing the victim to feel unsafe (Purcell et al., 2004). Some definitions require the victims themselves to feel threatened, whereas others require that a “reasonable person” would feel threatened (Blauuw et al., 2002a, Blauuw, Sheridan & Winkel 2002ap. 137). Some definitions require the stalker to intend to cause fear in the victim, and there is a differing minimum number of incidents for the behaviour to qualify as stalking.

Studies conducted before the Internet became widespread reported that a woman was 12–14% likely to be stalked over her lifetime, and a man was 4–7% likely to be stalked over his lifetime (Sheridan et al., 2003). Baum et al. (2009) estimated 3.4 million people in the United States alone had been stalked at some point during a 12-month period in 2005 and 2006. About 279,000 victims (over 8%) had been attacked by their stalker, 139,000 of which reported having been attacked with a weapon (Baum et al., 2009, p. 8). According to Meloy (2001, p. 16), violence in stalking cases is likely to be impulsive rather than premeditated, though this makes it no less harmful.

Spitzberg and Cupach (2007) identify several effects that stalking can have on a victim, which in addition to direct psychological harm may include secondary and tertiary effects to the victim’s social network. Increased anxiety and symptoms of Post-Traumatic Stress Disorder are common as the seemingly never-ending campaign of following and harassment continues, and many victims make major changes to their lives in order to cope (Pathé and Mullen, 1997).

In addition to direct psychological costs, coping with a stalker can get expensive. Costs associated with therapy and time taken off work can drain a victim’s resources, as can evasive measures such as moving house. It is common for friends and family to be abused by a stalker attempting to gain access to their primary target, causing social isolation. This isolation can be compounded if victims remove their social media accounts or change their phone numbers to escape persistent harassment.

The Internet age has brought about an unprecedented level of interconnectedness and convenience. The advances in communications technology have allowed friends and colleagues to keep in touch wherever they are in the world. However, this connectedness also allows a previously unimaginable level of personal information to be collected and disseminated, often without that person’s consent or knowledge.

This paper will survey the technologies used by stalkers in pursuit of their victims, as well as the technologies which can be used against stalkers. As there were very few technical papers (e.g. research that examines the security of the dating technologies such as websites and applications) concerning stalking found, this review was largely conducted by examining the stalking literature and further investigating any references to specific technologies. Papers were found by searching for “stalking”, “stalker”, “stalk technology”, “stalk surveillance”, “cyberstalking” and related keywords.

Similar privacy-intruding technologies such as those used by advertising companies and nation-state espionage groups were excluded unless the technologies were also able to be exploited by a stalker with technical knowledge but no special access to network infrastructure. Once technologies and techniques relevant to stalking had been identified, they were searched for using both academic databases and Google web search, in order to determine their technical capabilities and confirm that they had not been rendered obsolete by newer technology.

Similar literature reviews were conducted by Spence-Diehl (2003) and Southworth et al. (2007) on the topic of technology used by stalkers. Many of these technologies are still in common use by stalkers today, and some have advanced in the meantime. Spence-Diehl (2003)’s paper includes discussion of technologies used to keep victims in contact with counselors and advocates. Tokunaga and Aune (2015) study tactics used by victims of cyberstalking and develop a taxonomy of victim response behaviours. These tactics include ignoring the stalker, and “active technological disassociation”, meaning to use blocking features of the communications technology to keep the stalker from contacting them. This taxonomy of behaviours will overlap somewhat with the “Technology Used Against Stalkers” section of this paper, though approaching the topic from a different point of view.

2. Literature review

2.1. Stalkers

The academic community has categorised stalkers in several different ways.

A popular typology proposed by Zona et al. (1993) places stalkers into one of three categories: Simple Obsessional, Love Obsessional, and Erotomanic. Simple Obsessional stalkers have a prior relationship with their target, perhaps being an ex-lover, spouse or coworker. These are the most common cases (Meloy, 2001, p. 76). Love Obsessional stalkers often target celebrities or strangers in the hopes that the target will fall in love with them given enough contact. Erotomanic stalkers are similar to Love Obsessional stalkers, except the stalker has the delusion that the target is in love with them. The Erotomanic stalker is more likely to be female than the other two categories, which are more likely to be male (Meloy, 2001, p. 78).

Mullen et al. (1999) group stalkers into non-mutually exclusive categories based on their motivations: Rejected, Intimacy-seeking, Incompetent, Resentful, and Predatory. This typology approaches categorisation from a psychological perspective, and is intended for use in treatment of the stalker.

A more recent typology, and one better suited for the purposes of investigating the technological aspects of stalking, is RECON (Relationship and Context-Based), proposed by Mohandie et al. (2006). This categorises stalking cases based on the context of the stalking and the prior relationship of the stalker and target, placing cases in which the two have a prior relationship in one of “Intimate” and “Acquaintance”, and cases in which the two have no prior relationship in one of “Public figure” and “Private stranger” (Mohandie et al., 2006, p. 148). This typology addresses some concerns with the Zona et al. (1993) typology, such as the observation of stalkers transitioning
from the Love Obsessional category to the Erotomanic category (Mohandie et al., 2006, p. 147).

While every stalking case is different, there are many common behaviours seen over many cases, as reported by multiple studies (Brewster, 1997; Meloy, 2001; Pathé and Mullen, 1997; Spitzberg, 2002). Blaauw et al. (2002b) investigate the psychological impact to the victims when these features are present: listing the behaviours “Following”, “Damage of property”, “Direct unwanted approach”, ‘Surveillance of victim’s home’, “Unlawful entry in home”, “Threats to harm or kill victim”, “Physical assault”, “Sending letters”, and “Telephone calls” in roughly descending order of emotional damage. The features they mention are representative of the technology context at that time – for example the feature “Sending letters” is studied but there are no mentions of online behaviour.

The National Network to End Domestic Violence (2014) reported on the ways in which abusers misuse technology. The categories they identify are “Monitoring via Technology”, “Harassment via Technology”, “Impersonation via Technology”, “Tracking/Stalking via Technology”, “Non-consensual Pornography”, and ‘Abusing Children’s Technology’. The final category, ‘Abusing Children’s Technology’, refers to an abuser spying on their victim via their children, either by giving them technology such as a phone or laptop, or by gathering information from the child’s social media accounts. The report also lists the types of help abuse survivors are looking for: “General cellphone safety and privacy assistance”, “How to be safe online”, “Help around GPS/location tracking on phones”, “Technology and privacy issues associated with relocation”, “Getting personal information or images off the internet”, and “How to increase privacy when using computers or tablets” (National Network to End Domestic Violence, 2014, p. 5).

2.2. Technology used by stalkers

Many stalkers will conduct some form of surveillance on their target. In studies conducted before the rise of smartphones and the Internet, this surveillance is described as being surveillance of the victim’s home and following in public places (Blaauw et al., 2002b, Blaauw et al. 2002b, 55; Brewster, 1997; Meloy, 2001, p. 132; Pathé and Mullen, 1997).

As the technology has become more affordable to consumers, GPS (Global Positioning System) trackers have become more popular with people wishing to track their children, employees, or pets. These self-contained devices can be abused by stalkers to track their victims wherever they go, tilting the power dynamic of the relationship firmly in the direction of the stalker (Abbas et al., 2011). This dynamic has been described as “geoslavery”, and it enables the stalker to punish the victim for location infractions without requiring constant physical surveillance, coercing the victim into obeying the will of the stalker even in their absence (Dobson and Fisher, 2003).

A great deal of academic research on geolocation can be utilized by stalkers in pursuit of their victims. Li et al. (2014) investigate the location-based services WeChat, Momo, and Skout, and demonstrate that by setting up virtual devices with user-specified coordinates, a user can be targeted and their location triangulated. Hoang et al. (2016) investigate the LGBT dating apps Jack’d and Grindr, and demonstrate that users can be geolocated and tracked despite the privacy measures implemented by the applications. Carman and Choo (2017) examine geolocation using the popular dating service Tinder, describing an attack which can locate a user with greater accuracy than previous methods, despite the service’s security precautions. If the victim of an intimate-type stalker manages to escape their abusive relationship and tries dating again using one of these services, a stalker with enough technical knowledge can reacquire their location and renew the surveillance using these techniques.

It should be noted that not all academic research on geolocation is directly relevant to the stalker threat. Techniques for locating users which require a malicious or compromised location-based service, or which involve analysing large quantities of leaked data from such services, are unlikely to be utilised by a stalker; they require elevated levels of access, or a data breach which coincidentally includes the victim’s information. Research involving geolocating social media users by automatically analysing their posts for geographically specific keywords or analysing their social ties (Cheng et al., 2010, 2013; Rout et al., 2013) is also unlikely to be used in practice by a stalker who can look manually for such clues and gather a greater level of detail about the victim’s life in the process.

Spyware is a class of software which is installed on a computer or device, often without the legitimate owner’s knowledge, then logs and reports the owner’s activities to a remote party. These types of programs have been used by stalkers to monitor their victim’s computer usage, email accounts and passwords without their knowledge or consent, giving the stalker a great deal of power over them (Southworth and Tucker, 2006).

Hardware keyloggers are devices which are surreptitiously placed between a PC and its keyboard, and record all keystrokes typed into the computer. These devices are then either retrieved by the stalker, or the stored keystrokes periodically copied off the device using the PC. Modern spyware often includes a software keylogger feature, so the stalker can retrieve the keystrokes over the Internet.

As smartphones have become increasingly popular, a recent trend in spyware has been the mobile “stalker app”, with 54% of victim’s service providers having seen abusers tracking their victims in 2014 (National Network to End Domestic Violence, 2014). The term “stalker app” refers to a particular type of spyware available for mobile devices, whose primary purpose is to allow a user to covertly monitor a smartphone carried by another person. This class of software is marketed to people wishing to spy on their partners, children, or employees, and allows a user to view and control almost every aspect of their victim’s phone (U.S. Government Accountability Office, 2016). These tools allow for geographic surveillance via the phone’s built-in GPS, as well as the ability to view or block communication with the victim’s friends and family – their support network. Dang-Pham and Pittayachawan (2015)’s study indicates that mobile phone owners are less likely to lock their devices at home, leaving a stalker of the Intimate type a large window of opportunity to add such software. When installed without the knowledge of the victim, these apps provide invisible, real-time, remote access to a victim’s life, and give the stalker an almost omniscient appearance (Fraser et al., 2010, pp. 44–5). As a result they can make it very difficult for a victim to escape the relationship (Woodlock, 2013, p. 7).
As mobile phones are such an integral part of many victims’ lives, simply advising victims or potential victims of stalking to get rid of their phones is often unacceptable (Perry, 2012). Due to the ever-increasing number of stalking apps available to the public and the limited forensic capabilities of local law enforcement, it is very difficult for a victim to provide useful evidence if they do go to the police for help (Citron, 2015, p. 1249).

Webcams are available to consumers as standalone or USB-connected devices, as well as being part of most laptop computers and mobile devices. If a victim owns one or more of these devices, they can be compromised by a stalker and used to monitor, threaten or gather intimate photos or videos as blackmail fodder. Private Stranger-type stalkers with hundreds of “webcam slaves” have been caught and prosecuted in recent years (Anderson, 2013; Botelho, 2013). A privacy feature, the webcam indicator light which shows whether the webcam is active at the time, can in some cases be disabled remotely (Brocker and Checkoway, 2014) but is often not noticed anyway (Porthoff et al., 2015). A common privacy measure is to cover the webcam lens with tape to render it blind, but video chat and face-recognition applications are becoming more popular so the incentive to leave the webcam unobstructed is higher than in previous years.

Dedicated IP cameras may be accessible from the Internet if the owner uses the manufacturer’s default access credentials, or if there is a security vulnerability in the camera’s software. A security vulnerability may also allow a Private Stranger-type stalker to use the camera as an entry point into the victim’s network, from which they can attack the victim’s other devices. For example, security researchers from Cybereason demonstrated how (zero-day) vulnerabilities in IP cameras based on old Linux software from more than 10 different camera models and vendors can be exploited using a specially crafted HTTP request (Serper and Orot, 2017). These compromised cameras can then be used for spying and stalking. Devices which have not had security updates applied, either due to lack of an update mechanism or through neglect on the part of the user, continue to be affected past the point in which these vulnerabilities become public knowledge.

“Spy gear” stores sell hardware devices such as audio bugs, parabolic microphones and hidden cameras to would be spies. Modern eavesdropping devices can transmit over the cellular network or the AM/FM band, meaning that physical interaction by the stalker is not necessary once the device has been installed. Baum et al. (2009) estimate that 40.3% of stalking victims were monitored using hidden cameras, and 35.6% of victims were monitored with listening devices during a 12-month period between 2005 and 2006.

Drastic measures such as spyware are not necessary to monitor a victim. Burke et al. (2011)’s survey of undergraduates showed that approximately 25% of female students and 6% of male students monitored their partner’s private email accounts. In a study of Facebook users’ usage of the site, the motive “social surveillance” came second only to “keeping in touch with friends” (Joinson, 2008). The amount of data social media users willingly post about their lives and the existing culture of peer-surveillance make stalking behaviour almost routine (Levy, 2014, p. 689). Indeed, this behaviour has come to be known popularly as “Facebook stalking”, and has been studied by Lydon et al. (2011), finding the majority of survey respondents had engaged in some level of “Cyber Obsessional Pursuit”. McKeon et al. (2015) survey attitudes towards stalking, concluding that this type of obsessional behaviour, among other factors such as the perception of stalking as romantic, leads to attitudes of minimising and normalising stalking among the general public.

Facebook came under scrutiny in early 2015 after a Google Chrome extension named “Marauders Map” allowed users to retroactively view their friends’ movements due to location data leaked by the Facebook Messenger interface (Khanna, 2015). Facebook’s collection of these location data, never intended for display to their users, led to the privacy breach which affected the contacts of over 88,000 people who downloaded the extension. A stalker of the Intimate or Acquaintance RECON types could have used this opportunity to study the movements of their target in great detail.

Reverse image search sites such as TinEye and Google Image Search provide a service which allows users to search for a specific image and find copies elsewhere on the Internet (Williams, 2012, pp. 181–2). These tools have been exploited by stalkers to find a target’s social media accounts if the victim uses the same profile picture over multiple services. Dating blogs and magazines have posted guides to finding a target’s social media accounts online (Hogarth, 2014; Galore Girl, 2015), while the website stalkertools.com, dedicated to providing easy to use stalking guides, has posted entries containing the same techniques (Guerbuz, 2014).

“Human flesh search engines” are a Chinese phenomenon in which people in a forum-based community work together to answer queries and find people, using online and offline techniques (Wang et al., 2010). Using the skill of cyber-crowdsourcing, such activities (including netilantism) rely mainly on social networking platforms on which other online users may unwittingly provide information and clues about the victim. In 2008, a man successfully used one of these communities to find his ex-girlfriend, whom he then stabbed to death (Wang et al., 2010, p. 47).

Similarly, Internet commenters in pursuit of a political or ideological agenda have been known to “dox” their opponents – that is, creating a dossier of information about the target gathered from public sources and releasing it in order to allow for more efficient harassment, such as the allegations relating to the most recent U.S. election reported in a number of media outlets (see Lipton et al., 2016). While the initial data-gathering act may not necessarily be categorised as stalking, the resulting campaign of harassment might appear similar from the victim’s perspective, and afterwards a stalker may use these data for their own purposes. The obvious differences between the doxing phenomenon and classic cases of stalking are that typically multiple people are working together, and the motivation is to silence the target and win an argument by attrition, rather than keep the dialogue open.

Harassment of the target is a common feature of stalking behaviour. While studies conducted before the widespread availability of the Internet showed high percentages of cases in which telephone calls to the target were present (Blaauw et al., 2002b), stalkers in the Internet age have a wider variety of communication channels at their disposal (Haron and Yusof, 2010). In addition to the telephone network, harassers can make u-
sance phone calls using VoIP technology. This technology allows a user to easily spoof their outgoing phone number, bypassing caller ID and number blocking systems (Hatifled, 2010). As a result, victims are often forced to get a new phone number, and limit who they give the new number to. Dimond et al. (2011, p. 418) describe two women who lost contact with their families after their sisters repeatedly gave out their new phone numbers to their stalkers. Victims of repeated harassing calls are likely to stop answering their phones, further isolating them from their support system (Woodlock, 2016).

Social media can be abused by stalkers to send harassing messages, as well as by posting humiliating photos or stories. Victims who delete their social media accounts, especially teenagers, risk losing social capital (Ahn, 2012).

Bluetooth, and related services such as Apple’s AirDrop, allow nearby smartphone and laptop users to transfer files to one another. This has been abused in at least one case of “cyber-flashing”, an incident in which an unknown person sent indecent photos to a woman while travelling on a train (Bell, 2015). A stalker given temporary access to a victim’s smartphone might also be able to abuse these features in order to send the victim’s sensitive files to their own device. In addition, a victim might be tricked into installing a malware on the device that facilitates subsequent spying or stalking.

When a victim relies on the Internet for a living, stalkers have a classic hacker’s technique for causing trouble: the Distributed Denial of Service (Fagone, 2015). Services which utilise networks of compromised computers around the world allow even novice Internet users to pay a fee and flood a particular network address with online traffic, meaning that legitimate network connections to and from the victim will slow to a crawl or stop altogether.

Email and chat services can be abused by stalkers to send many messages to a victim at all hours of the day, or by posing as the victim and soliciting sexual acts from strangers (Lamberg, 2001; Southworth and Tucker, 2006). The victim can also be impersonated with the goal of getting law enforcement involved. There is a case in the literature of a stalker using his victim’s compromised email accounts to falsify threats to him, which he then took to the police as evidence against her (Southworth and Tucker, 2006).

A similar phenomenon is that of “swatting”, in which an individual falsely reports a crime at the victim’s home in order to provoke an armed response by law enforcement. This usage of highly militarised police departments as a weapon first appeared in 2008 (FBI, 2013) and became popular in the online gaming scene as an intimidation tactic. Swatting is a tactic used by both Private Stranger (Fagone, 2015) and Public Figure (Lee and Winton, 2012) stalker types. If the victim is part of the online streaming community or they have a hacked webcam, the stalker gets the instant gratification of watching the live video stream as the victim is raided by the police (Wingfield, 2015). Stalkers conducting swatting can abuse Caller ID spoofing (FBI, 2013) or telecommunication devices intended for the hearing impaired (Krebs, 2013; Southworth et al., 2005, p. 6) in order to make their hoaxes more believable and harder to investigate.

A recent and disturbing trend is the rise of “non-consensual pornography” – the publishing of sexual photos and video without the victim’s knowledge. The widespread dissemination of these images is made simple by specialised websites which allow users to upload these images as well as links to the victim’s social media accounts and personal details. Compounding the emotional damage to the victim is that these websites are indexed by search engines such as Google, meaning that a search for the victim’s name by a friend or potential employer will return the photos. The academic literature focuses on the legality of posting these media and of taking them down (Burris, 2014; Cecil, 2014; Citron and Franks, 2014; Levendowski, 2014; Stokes, 2014), which is complicated by free speech laws.

The technologies used by stalkers are summarised in Table 1.

2.3. Technology used against stalkers

There appears to be a large literature gap concerning the use of technology to deter or detect stalking. Dunlap (2012)’s review

---

**Table 1 – Summary of technologies used by stalkers.**

<table>
<thead>
<tr>
<th>Technology</th>
<th>Monitoring</th>
<th>Tracking</th>
<th>Harassment</th>
<th>Impersonation</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPS trackers</td>
<td></td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Keyloggers</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hidden cameras</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Webcams</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audio bugs</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Long-range microphones</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telephones/VoIP</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Location-based dating apps</td>
<td>Yes</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Spyware</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Mobile stalker apps</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Online email accounts</td>
<td>Yes</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Social media</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Marauders Map</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Reverse image search tools</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human flesh search engines</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bluetooth/AirDrop</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Distributed Denial of Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email/chat</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-consensual pornography websites</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
of stalking’s relationship to technology shows a vast disparity between technology used by stalking and technology used against stalkers, the latter largely being used to track offenders by law enforcement. This tracking of convicted offenders, usually via a transmitter securely attached to the offender’s ankle, can of course only be used after the victim has suffered through both a period of stalking and a trial, so while it will surely provide some comfort to the victim, the psychological damage may have already been done.

Antivirus apps are available for mobile devices, and will detect stalker apps if the antivirus vendor has included appropriate signatures in the software. However, antivirus vendors may not add these signatures, as the industry does not necessarily class these apps as malware (Kirschner, 2013). Applications available on the Google Play Store claim to use heuristics and signatures to detect spyware on Android devices (skibapps, 2016), but it is unknown how effective these apps are in practice. For example, in two related studies of free anti-malware apps for Android devices by Walls and Choo (2015, 2016), it was found that the effectiveness and reliability of these apps significantly varied across different Android operating systems and hardware test devices.

Users can also jailbreak or root their devices to bypass the security measures implemented by the manufacturer. Root access allows a stalker app installed on the device to view and change data that would otherwise be protected by the operating system, expanding the capabilities of the app. Jailbreaking devices running iOS makes it possible to install applications not on the App Store, which have not been vetted by Apple and may be malicious. However, rooting also allows the user to install software such as firewalls and privacy guards, giving them greater ability to block apps from accessing the Internet or private data stored on the device.

Mazhelis and Puuronen (2007) propose a framework for the detection of unauthorised users of a mobile device. This framework uses biometric factors such as typing quirks and gait, as well as factors such as the speed at which the user comprehends blocks of text shown on the screen, in order to allow the device to detect that it has changed users and respond accordingly. As stalker apps are very quick to install, this type of system will likely not have gathered sufficient data to make a conclusive judgement about the user’s legitimacy. Biometric locks such as fingerprint sensors are now seen on many modern phones, and make unlocking the phone much simpler for legitimate users, while preventing unauthorised users from easily accessing the device without the owner’s knowledge.

Recent versions of Android and iOS allow the user to encrypt the data on the device. If the device is stolen by the stalker and they attempt to use forensic techniques to read data from the internal memory or SD card, they will first require the victim’s password.

Chen et al. (2015) propose a simple method for detecting unusual behaviour of mobile devices which analyses the network traffic generated by the device, looking for HTTP requests containing personal information and using Whois requests to determine the recipient. This method is a good start, however the simplest of encryption algorithms employed at application level or usage of a protocol other than unencrypted HTTP will allow malware to remain undetected by this method.

In addition the proliferation of virtual hosting means that attribution of a server is not always possible – a piece of malware using the same virtual provider as a legitimate service may be marked as normal traffic. A wireless hotspot which conducts similar network examination of a mobile device has been patented by Wu (2013).

A browser extension for the dating website OkCupid builds on research by Lisak and Miller (2002), allowing users to easily spot potential sexual predators based on a number of “red flag” questions (Meitar, 2013). This extension by its nature can only detect users who voluntarily answer questions regarding past sexual violence in the affirmative, and as such will not identify users who aren’t as blatant when answering their match questions.

al-Khateeb and Epiphaniou (2016) discuss the automated detection of online predators in chat rooms using machine learning, identifying malicious users by the language they use. This research may be useful for chat room administrators or law enforcement.

Anonymity network Tor allows users to bounce their Internet connection over multiple encrypted nodes across the world. This makes surveillance of a Tor user’s Internet connections very difficult – a system watching the network will see encrypted connections to Tor servers, but the end connections will appear to have come from completely different Tor servers, somewhere around the world. Shelters housing women who have fled from their abuser have been known to use Tor to keep the location of the shelter secret (LeVines, 2014), though this may in fact put its clients at risk for little benefit. McCoy et al. (2008) and Chakravarty et al. (2011) have investigated Tor exit nodes for monitoring of cleartext traffic. McCoy et al. (2008) used the reverse DNS feature of packet sniffing software tcpdump to detect whether that particular program was monitoring the network traffic at the exit node. Chakravarty et al. (2011) set up a decoy mail server and connected to it repeatedly over Tor, waiting for others to connect using the same credentials. Both studies found instances of monitoring, indicating that the Tor network is not safe for cleartext traffic. The “Private Stranger” stalker type may indeed find a target by abusing Tor – exit nodes can be set up for free and will allow a stalker to view Internet connections from users around the globe, collecting usernames and passwords for unencrypted services (McCoy et al., 2008) and using them to break into more valuable websites due to password reuse. It is unlikely that an existing victim of a stalker will unwittingly supply their login credentials to that stalker directly, but their details may end up on one of many lists bought and sold online (Krebs, 2012). Meanwhile, the technical knowledge and access required to physically locate a victim’s shelter by their Internet address makes this a very difficult proposition for a stalker, especially as IP address geolocation – protection from which is the main advantage of Tor – is usually limited to the ISP and city the address is assigned to, and in many cases these services are unreliable (Prieditis and Chen, 2013; Triukose et al., 2012). When used by a women’s shelter, this anonymity vs confidentiality tradeoff may not be in the clients’ best interest, and the shelter would likely be better served by employing an offshore Virtual Private Network (VPN) instead.

Tor may be used by anonymous stalkers to conceal their IP address when making contact with their victim. However,
in practice this is unlikely to yield significant advantage unless law enforcement is conducting an investigation. Most modern communication channels which could be used to harass a victim involve one or more servers which act as middlemen for the message and do not distribute the sender’s IP address for privacy reasons. Victims attempting to identify such a stalker without law enforcement help have less technical options available to them, such as analysing the content or metadata of messages sent by the stalker for clues as to their identity, neither of which will be affected by the stalker’s usage of Tor.

Perry (2012) has written a guide to the technology risks victims of stalking may face, and provides helpful, user-friendly tips for protecting one’s privacy and safety in the face of this type of adversary. Blue (2015)’s guide to privacy for women gives advice for preemptively keeping personal information out of the hands of potential stalkers. Tokunaga and Aune (2015) study the tactics victims of cyberstalking use to attempt to manage their risks, identifying the themes “Ignore/avoidance”, “Active technological disassociation”, “Help seeking”, “Negotiation/threat”, “Compliance/excuses”, “Technological privacy maintenance”, and “Derogation”.

A summary of technologies used against stalkers is presented in Table 2.

### Table 2 – Summary of technologies used against stalkers.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Effective against</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPS ankle monitor</td>
<td>Physical following by convicted stalker</td>
</tr>
<tr>
<td>Smartphone fingerprint lock</td>
<td>Discreet installation of stalker apps</td>
</tr>
<tr>
<td>Antivirus</td>
<td>Spyware, stalker apps</td>
</tr>
<tr>
<td>Specialised stalker app detection software</td>
<td>Stalker apps</td>
</tr>
<tr>
<td>Firewalls</td>
<td>Spyware, stalker apps</td>
</tr>
<tr>
<td>Privacy guards</td>
<td>Spyware, stalker apps</td>
</tr>
<tr>
<td>Device encryption</td>
<td>Device theft</td>
</tr>
<tr>
<td>OkCupid Predator Alert Tool</td>
<td>Potential predators using online dating</td>
</tr>
<tr>
<td>Tor anonymity network</td>
<td></td>
</tr>
<tr>
<td>Virtual private networks</td>
<td></td>
</tr>
</tbody>
</table>

3. Discussion

There is a need for technologies which empower victims or potential victims to take a more active role in addressing their own stalking. Stalkers use technology to appear in the victim’s eyes as omniscient, seemingly aware of everywhere the victim goes and everybody they speak to (Fraser et al., 2010). Technology which can demystify the nature of a stalker’s surveillance while simultaneously gathering evidence of it will start to shift the balance of power over to the victim’s side, putting a would-be stalker on the defensive.

The capabilities and motivations of a stalker differ from that of an institution such as an advertising company or government agency. These differences can explain why existing technologies whose adversary model resembles one of these institutions are often ineffective against the stalker threat, and understanding them is critical to developing useful anti-stalker tools. For example, most stalkers do not have the technical resources or financial support of an organisation or government while conducting their surveillance. Unless they have privileged access to their victim’s device (e.g. mobile phone) or data as part of one of these institutions, they will need to take a very different approach to successfully track their victim. However, a stalker has an advantage over institutions conducting mass surveillance in that they are tracking a comparatively small number of victims, so the amount of data that will need to be analysed can be done manually rather than relying on automated processes. Stalkers have the option of utilising time- and labour-intensive spying methods which would become prohibitively costly if implemented at large scale by an institution attempting to surveil massive numbers of people.

Once a victim has become the target of a stalker, simply blocking a certain class of tracker will not end the surveillance. While, for example, a company’s tracking of an individual customer using a loyalty card can be stopped by refusing to present the card, a stalker is by definition obsessed with their victim and can renew the surveillance through other channels.

The data gathered by institutions need to be largely machine-readable for efficient processing. Conversely, data gathered by stalkers should be of a form intelligible and useful to an individual person. Attempting to alert the user when sensitive data are exfiltrated from a smartphone, Chen et al. (2015) specify these data as being device identifiers such as the phone’s IMEI (International Mobile Equipment Identity) and IMSI (International Mobile Subscriber Identity) numbers, the operating system version, and the contents of the address book. While a list of the victim’s friends, family and acquaintances could be incredibly valuable to a stalker, technical details such as IMSI numbers are likely to be useless to them. A text string such as “see you in 30”, exfiltrated from the victim’s sent text messages via a stalking app, would be very difficult to programmatically detect by using this type of analysis but would indicate a major breach of the victim’s privacy.

Technologies developed to detect surveillance by stalkers may have the potential to be abused by those attempting to evade surveillance by law enforcement, much in the same way that many existing privacy and security technologies can be abused by criminals to hinder investigations. Knowing the differences between stalker and law enforcement capabilities and procedures will enable researchers to develop techniques in a way which maximises effectiveness against the stalker threat while offering minimal utility as an anti-law enforcement tool.

For example, law enforcement has a wider range of surveillance capabilities, as while stalkers are largely limited to consumer products and public-level access to services, law enforcement has the ability to use legal channels to compel data from third parties such as social network providers (e.g. https://www.facebook.com/records/x/login/) and search engines (e.g. Google Transparency Report on https://www.google.com/transparencyreport/userdatarequests/legalprocess/). When conducting physical surveillance of a suspect, law enforcement is able to cycle through multiple personnel in order to avoid detection, and can utilise surveillance camera feeds unavailable to the general public. Law enforcement can also communicate using specialised radios, rather than relying on the civilian phone network. Anti-stalking technology, devel-
oped under the assumption that the stalker is working alone and using publicly available tools, is unlikely to be inadvertently useful against these law-enforcement surveillance techniques.

Blaauw et al. (2002a) showed that victims of stalking in which the stalker conducted surveillance had a GHQ-28 General Health Questionnaire (Goldberg and Hillier, 1979) score 2.2 points higher than victims of stalking for which surveillance was not present. This statistic indicates that providing counter-surveillance options to potential victims of stalking may have a large positive impact on their mental health.

Research avenues will likely take one of three forms. The first is improving existing anti-stalker technology, possibly by making it cheaper, easier to use or more reliable. The second is developing technology to counter existing stalker technology by detecting its presence or by impeding it in some way. The third is developing new technologies which counter stalking behaviours, not necessarily only those behaviours which use specialised technology.

There is potential for improvement of existing tools. For example, the OkCupid Predator Alert Tool relies on a potential predator to answer one or more “red flag” questions truthfully. These questions are not particularly subtle, and while they may detect predators who have admitted to sexual assault or other predatory behaviour, they will not detect predators who have skipped these questions or have lied. A study of users’ responses to other questions and how they correlate to the red flag questions may prove to identify characteristics of predators which are not as obvious. OkCupid has a history of conducting similar analyses, with the OkTrends blog (Rudder, 2014b) and book Dataclysm (Rudder, 2014a) discussing many.

The Tor research conducted by McCoy et al. (2008) and Chakravarty et al. (2011) can be extended by connecting to insecure web services using Tor and checking for access attempts to other well-known services using the same credentials. These attempts can be detected by enabling the two-factor authentication option, meaning that a message will be sent to a mobile device or email account in response to the credentials’ entry into the service.

The most effective piece of surveillance technology available to a stalker is surely a discreetly installed smartphone app. These applications are designed to be difficult to find during normal operation, hiding from operating system menus and using inconspicuous or technical-sounding names. This strategy makes the apps unlikely to be found and removed until after the stalker reveals some piece of information which indicates that the victim’s device has been compromised.

Detecting individual stalker apps using signatures, as an antivirus program would, requires the user to install scanning software ahead of time and regularly conduct scans, potentially draining precious battery life and risking being manually disabled by the stalker. If the scanning software is not installed before the stalker app, the process of finding and installing the scanning software is likely to be detectable by the stalker app, and the stalker may be able to retaliate before their app is found and removed.

An alternate method for detecting stalker apps could build on existing work conducted by Chen et al. (2015). Rather than searching for specific strings in a network packet capture in an attempt to detect the exfiltration of sensitive data, this research could focus on detecting apps specifically designed to facilitate stalking. By focusing on a single class of applications, a more resilient set of heuristics can be developed which will additionally exclude the routine and non-threatening privacy violations such as those conducted by mobile advertising companies.

Stalker apps can be actively probed by sending emails, SMS and social media messages, and by browsing the Internet on the device, in order to get the app to exfiltrate known data via the network connection. These apps could also be detected passively by a device installed long-term on the local network, allowing concerned third parties such as parents or employers to ensure no devices on their network have been compromised. While the similar research conducted by Chen et al. (2015) will be foiled by an encrypted network connection, this process should focus on the entropy and metadata of the device’s connections, preserving the device owner’s privacy and identifying suspicious traffic irrespective of whether encryption has been employed by the stalking app.

The amount of information on a person accessible with just a quick Google search is so well known that the process is known as “Google-stalking” (Van Roekel et al., 2006, p. 74). Stalkers can use a series of search queries to find all of their targets’ usernames, email addresses and online postings, with virtually no chance of being caught. Various “people search” websites exist which conduct this investigation automatically and combine the results with public record data to provide a dossier on an individual given only a name and location (Truman, 2010, pp. 19–20). Future research can be conducted into tools and techniques to make this process more difficult and less fruitful, or at the very least, traceable.

Detecting whether an Internet user has searched for a specific person’s name is unlikely to be possible using tools such as Google Trends, as they typically enforce a minimum search count before trend data are shown.

Research has been conducted on Search Engine Optimisation, which may be extended to create false trails and identities in order to reduce the reliability of Google searches for a certain individual’s personal information. Such research could be used to create a tool which allows victims of stalking to take certain pieces of personal information such as location or contact details, and force a Google search to return false information when a stalker attempts to find out these data. The same tool could also include a honeypot component and send alerts when the false data are accessed. Alternately, the concept of an “online identity” could be blurred by creating records which tie the stalking victim’s name to account names of people with similar details. This work would likely be most useful for an individual evading a Private Stranger stalker’s investigation, but could also be useful when attempting to escape an Intimate or Acquaintance stalker type.

Google stalking usually involves searching for a victim’s full name in order to find their public online accounts and any usernames or aliases they use regularly, then searching for these usernames and aliases to find more uses of them which may not have been linked to the victim’s full name. As people tend to reuse the same usernames on different websites, this process
is very effective, but it relies on the accuracy of these search results and so is vulnerable to manipulation.

The Google Reverse Image Search tool can be used by stalkers to link together social media accounts without any commonalities other than a reused photograph or avatar. A research project which generates distortions of a specific image, which cannot be connected to each other, can be applied to a person's profile picture. Unique distortions uploaded to each social media account would foil this type of Google stalking. This concept is similar to the CV Dazzle project by Harvey (2012), in that it involves disrupting of computer vision to protect a person's privacy, though it targets a different class of algorithms to that project.

The technology used by a stalker is not limited to stalking technology. Common devices such as smartphones can be detected from a distance using protocols such as Wi-Fi and Bluetooth.

Shoppers in large malls may be subjects of surveillance of their mobile devices, which can be used to track them as they move through stores (Michael and Clarke, 2013). These “footfall” tracking systems comprise many detectors, collecting the unique device identifier sent out regularly by WiFi-enabled devices to determine whether any known networks are nearby. In an effort to combat long-term collection of these data, many new phones and PC operating systems randomise this identifier while searching for networks, and/or for each new network connection (Vanhoef et al., 2016). However, devices conducting this randomisation can often still be tracked by fingerprinting the lower-layer attributes of the device, by using active attacks or by keeping track of sequence numbers over time (Freudiger, 2015; Vanhoef et al., 2016).

There exist many publications covering the tracking of moving targets using multiple fixed sensors (Li et al., 2014, 2015; O’Connor, 2013; Zhou et al., 2014) which make that research primarily useful for private companies who wish to learn more about their customers’ movements, or law enforcement agencies who wish to conduct mass surveillance of an area. These entities have the financial resources and legal authority to mount permanent or semi-permanent sensors over a large area. O’Connor (2013)’s research was aimed at private individuals such as stalkers – the sensors were specifically designed to be cheap and disposable, with decentralised command and control and built-in anti-forensic measures. This research could conceivably be used by a stalker in any of the RECON categories by planting sensors in strategic locations where their target could be expected to visit.

While counter-surveillance tactics which may help victims of stalkers using these types of techniques have been implemented by new mobile devices, this research can also be extended to actively detect physical surveillance with a single detector carried by the victim as they go about their daily routine.

The biggest challenge with this research is likely to be identifying attributes of following behaviour which differentiate malicious following and inadvertent or coincidental following. Some example attributes which might be useful in calculating how threatening a device is would be whether the device is connected to a local wireless network, indicating that the device owner probably belongs in the area; the length of a single device’s follow event significantly exceeding the crowd average, indicating that the device owner is alone and moving with the sensor; and a device being seen in multiple different contexts, for example at the user’s home, work and shopping centre.

4. Conclusion

Since the widespread proliferation of the Internet, stalking behaviour has adapted to involve modern technology in a majority of cases (National Network to End Domestic Violence, 2014). There is a staggering amount of technology currently in use by stalkers to monitor, track, harass, impersonate, and humiliate their victims. Twenty years ago, to find out a person’s movements one had to stake out their home and follow them throughout their day until they returned. Now, all a would-be stalker needs to do is borrow their victim’s mobile phone and they can pinpoint their location wherever they go, listen to any conversation they have, and read any email they receive. Stalkers without access to their target’s mobile phone can purchase hardware trackers and microphones very cheaply.

People living on the other side of the world can use the webcam installed in a modern laptop to blackmail its owner into conducting sexual acts on-camera, and manage hundreds of such victims at a time. These technologies have made stalking easier, faster, more cost-effective, and they provide a level of detail on a victim’s life unmatched by traditional stalking methods.

The technology available to detect or deter stalking pales in comparison. Antivirus protection for mobile devices, if used at all, often ignores stalker apps either due to policy or lack of signatures. Network examination software proposals are trivial to evade by using HTTPS rather than HTTP, and will also flag advertising spyware, resulting in a high number of false positives in the stalking context. Apps which aim to detect potential sexual predators require them to state that they have previously sexually assaulted somebody, or have troubling views on consent.

Technological measures implemented by legitimate services to counter stalking are largely defensive and reactionary in nature. Social media websites offer the ability to block certain accounts, and modern phones can block certain numbers, but a determined stalker will simply use a different account or phone number. These reactive solutions can temporarily address harassment, but cannot be employed if the victim does not know how, or even if, they are being stalked.

General security technologies designed to defend against a wide variety of threats, such as firewall and antivirus applications, provide some protection against stalkers utilising technical means to invade their victim’s privacy. However, to protect against the more specific threat of stalking, new techniques must be developed and implemented.

Future research agenda includes improving existing privacy and anti-stalker techniques, such as by identifying a set of more innocuous dating site questions that correlate with Lisak and Miller (2002)’s red flag questions or testing existing “stalker app detector” software against popular stalker apps; and developing techniques to detect covert stalking behaviour on social
media and blogging platforms, which can act as an early warning system for potential victims. Also, one of the reviewers suggested that addressing the cyber harassment of disabled people is important, as “such vulnerable group might require special technology to facilitate their response to online stalking and harassment.”

Acknowledgements

The authors thank the Associate Editor and the five anonymous reviewers for their constructive feedback. The second author is supported by the Cloud Technology Endowed Professorship.

References

Brewster MP. 1997, An exploration of the experiences and needs of former intimate stalking victims, final report submitted to the national institute of Justice. 
Cecil AL. Taking back the internet: imposing civil liability on interactive computer services in an attempt to provide an adequate remedy to victims of nonconsensual pornography. Wash Lee L Rev 2014;71:2513–56. 


Hoang NP, Asano Y, Yoshikawa M. 2016, Your neighbors are my spies: location and other privacy concerns in dating apps, in 2016 18th International Conference on Advanced Communication Technology (ICACT), IEEE.


O’Connor B. 2013, CreepyDOL: cheap, distributed stalking, BlackHat.


Rudder C. Dataclysm: who we are (when we think no one’s looking). New York, NY: Random House Incorporated; 2014a.


Rudder C. Dataclysm: who we are (when we think no one’s looking). New York, NY: Random House Incorporated; 2014a.


Rudder C. Dataclysm: who we are (when we think no one’s looking). New York, NY: Random House Incorporated; 2014a.


Rudder C. Dataclysm: who we are (when we think no one’s looking). New York, NY: Random House Incorporated; 2014a.


