Northern Illinois University
Huskie Commons

Honors Capstones | Undergraduate Research & Artistry

1-1-2016

University Policies on the Dangers of Spyware Apps

Julia L. Boyle

Follow this and additional works at: https://huskiecommons.lib.niu.edu/studentengagement-honorscapstones

Recommended Citation
Boyle, Julia L., "University Policies on the Dangers of Spyware Apps" (2016). *Honors Capstones*. 1355.
https://huskiecommons.lib.niu.edu/studentengagement-honorscapstones/1355

This Dissertation/Thesis is brought to you for free and open access by the Undergraduate Research & Artistry at Huskie Commons. It has been accepted for inclusion in Honors Capstones by an authorized administrator of Huskie Commons. For more information, please contact jschumacher@niu.edu.

NORTHERN ILLINOIS UNIVERSITY

University Policies on the Dangers of Spyware Apps

A Thesis Submitted to the
University Honors Program
In Partial Fulfillment of the
Requirements of the Baccalaureate Degree
With Upper Division Honors

Department of
Communication
By
Julia Boyle
DeKalb, Illinois
May 2016

ABSTRACT: Despite the comprehensive nature of many universities' cyberstalking policies, the rapid rate of technological growth has created legal loopholes. The growing popularity of unregulated spyware apps--typically marketed towards employers and parents, has fallen into the hands of abusers, creating an innovative outlet to easily stalk victims. Domestic violence shelters are increasingly receiving young victims who have been stalked by spyware apps. Thus, by analyzing the cyberstalking policies of three top universities, this study will seek to discover the effectiveness of fighting against those perpetuating violence through spyware apps. Finally, in comparison with the three schools, Northern Illinois University's policy will be analyzed.

At the turn of the twenty-first century, mobile phones were expected to peak in relevancy, only to fade into obscurity. The evolving nature of the technology, however, surpassed even the top executives of the first mobile phone manufacturing companies. To date, mobile phones outnumber people in the United Kingdom, and it is projected that there will be 50 billion mobile devices worldwide by 2020 (Wray, 2009). We as a society have evolved with the popularity of mobile devices. Dependency is so prevalent within people to their mobile devices, that many young individuals report a feeling of fear without it near them at all times, or "nomophobia." Cell phone users rely so heavily on the ubiquitous ways of using this medium of communication that they rarely go without their phones.

Of course, with any quick evolution of technology comes the risk of abuse. Smartphone technology grants its users to download and customize applications on their phone. The creative nature of apps allows more advanced users to create their own. The dependency of mobile devices enables abusers to install exploitation into their victim's extension of self. Spyware apps are quickly becoming the newest, legal way to stalk a victim's mobile device without them ever knowing. Although 85% of domestic abuse shelters have worked directly with victims who have been stalked by spyware apps, advocates remain improperly trained due a lack of knowledge of the apps' existence (Shahani, 2014).

While cyberstalking policies are commonplace in university policy, the advanced evolving nature of mobile technology do not address new mediums of abuse such as spyware apps. In this paper, I will explore how universities have addressed the threat of spyware apps among young people. Through outlining how spyware apps work, their prevalence and use, and current legislation, my research among university policies can offer insight on how to remedy this technological plight.

LITERATURE REVIEW

Stalking has been viewed as a societal issue by legislators only since the 1990s, according to the Stalking Resource Center (2003). However, few could have anticipated the legal minefield that technology has produced, thus leaving cyberstalking victims legally uncovered. In 2003, the Stalking Resource Center reported that all 50 states have stalking policies, but only 1/3 of states cover cyberstalking (p. 1). California, for example, constitutes cyberstalking only through a credible threat that is "verbal, written, or electronically communicated statements and conduct" (p. 1). The broad language of laws does not protect victims who are being stalked in

unique, intrusive forms. The Stalking Resource Center urged individuals to contact state representatives to review the language of their cyberstalking laws in 2003. Yet, the Stalking Resource Center could not have possibly fathomed the extent to which cyberstalking would evolve.

Tragically, technology has been used to exploit and violate individuals for over a decade. Preliminary research from Calman (2005) illustrates the threat of spyware technology on shared desktop computers. Services such as SpectorSoft, which allows parents to take screenshots of their children's activity on the computer, have been in existence since 1999 (2005, 2100). Advertisements for stalking apps typically target employers and parents to monitor their employees and children, yet they do not make up the majority of the market. Over 40% of spyware was purchased with the intention to stalk a domestic partner by 2002 (Calman, 2005). Similar to spyware app technology, Calman warned individuals that their partner might be monitoring their activity on a shared computer (2005, p. 2097). A person utilizing spyware may record all Website history, instant messages, and overall keystrokes—all without their partner ever knowing.

While spyware became a more identifiable threat with awareness, spyware apps came into existence shortly thereafter. Southworth & Tucker (2007) assert that spyware was no longer limited to desktop and laptop computers as early as 2006 (p. 669). The first spyware app, FlexiSpy, debuted in 2006 to "monitor kids and unfaithful spouses" (Southworth & Tucker, 2007, p. 669). As advertisers became more transparent about the apps' potential use, the technology has steadily risen. Cell phones allow an abuser to micromanage a smaller device, and monitor each and every keystroke (Southworth & Tucker, 2007). Southworth & Tucker explain that while phone companies may have access to call records, there are no guarantees that they can connect the crime to the perpetrator, making cell phones the most viable option to stalk (2006, p. 673).

Regardless of a seemingly universal definition of stalking, the act was not criminalized until 1990 (Campbell & Moore, 2011). The nature of stalking can be mysterious and difficult to distinguish for the victim. Products of stalking often cannot be proven as illegal criminal offenses, such as threatening e-mails, texts, or calls (Campbell & Moore, 2011). Even more troubling, Campbell and Moore report that some victims may perceive jealous and threatening byproducts of stalking to be typical in a romantic relationship (2011). Thus, legitimate statistics

on those who have reported stalking is murky at best. To date, these numbers are climbing. College students, although equipped with the knowledge to identify stalking, are most likely to be stalked by a romantic partner (Campbell & Moore 2011).

Although spyware apps have been in existence for years, even the most prevalent stalking resources do not comprehensively cover resources for spyware apps. The Stalking Resource Center addresses spyware on computers (2012). When addressing spyware apps on computers, The Stalking Resource Center primarily asserts that Caller ID spoofing is the problem; the only link on spyware apps is not a useable link (2012). However, in 2012, spyware apps were simultaneously picking up traction in other areas. The year 2012 introduced Minnesota Senator Al Franken's bill, The Location Privacy Protection Act in an attempt to ban spyware apps (Ramasastry 2012). Although Franken's bill has the capacity to assist the multitude of victims affected by spyware apps, not everyone bought its appeal. Ramasastry notes that telecommunications departments found Franken's bill to be harmful for app innovation, and virtually impossible to pass (2012).

Franken then attempted to pass the bill once and for all in 2014, calling it "commonsense" (Franken, 2014). To please telecommunication critiques, Franken attempted to remedy the issue by addressing corporations in the bill (Franken, 2014). To date, his bill has not passed. Simultaneously, NPR interviewed the aforementioned Cindy Southworth, an advocate with the National Network to End Domestic Violence to expose the gravity of spyware apps in an innovative investigative report. Southworth asserts that our national concern with technological privacy and the government is short sighted (Shahani, 2014). Abusers utilize spyware app technology to perpetuate a power complex on their victim; spyware apps go beyond just the scope of surveillance (Shanhani, 2014). Unlike just watching a victim's activity through a computer, the abuser has the option to control who the victim calls, log their messages, and hold them accountable with this information. NPR found that cyberstalking is now ingrained in domestic violence in the US (Shahani, 2014).

In response to the NPR investigative report, many media outlets, such as CBS explored the legal repercussions these apps. CBS covered the arrest of Hammad Akbar, creator of the spyware app StealthGenie for his illegal activity (Dahl, 2014). Akbar bragged that StealthGenie is "100%" undetectable" on their partners phone (Dahl, 2014). Dahl explained that the arrest of Hammad Akbar started a dialogue about Minnesota senator Al Franken's Bill, which would ban

GPS location-based spyware apps (2014). Despite the author's idealistic intent, the bill has not been passed. Advocates such as Cindy Southworth are more skeptical of Akbar's arrest, explaining that there are hundreds more of undocumented spyware apps (Dahl, 2014).

Most recently, Knibbs (2015) harshly critiqued the legal system for a lack of action on spyware apps. Increased awareness of spyware apps has sparked a dialogue, but has inspired little legal action. Knibbs explains that apps such as mSpy and flexiSPY have had millions of downloads to date, according to their sales figures (Knibbs, 2015). Vague legal language still attempts to justify the spyware as intended employee and children use, yet mSpy stats indicate that 45-50% of users are utilizing the technology for "other" reasons (Knibbs, 2015). Because the potential for abuse is so apparent, mSpy has actually readjusted its policy to have stalkers identify as employers or parents in order to escape legal loopholes (Knibbs, 2015). Knibbs argues that law enforcement continues to be lax on the issue, which illustrates privacy issues within our own government (2015).

HOW SPYWARE APPS WORK

The scope of spyware apps is rather astounding. Although hundreds of undocumented apps are not available through mainstream downloading sources, like the App Store, two apps can be noted as the top performers. Both mSpy and flexiSPY are estimated to have millions of users, according to their sales figures (Knibbs, 2015). The downloading process of these apps are relatively cheap—and simple.

Similar to any subscription, these apps require the user to pay a small fee. mSpy, for example, costs $70 a month, or $200 a year (Shahani, 2014). The downloading process can take about of minute to install on a person's phone, preferably jailbroken, or the process of removing restrictions on an iPhone. A person may feel comfortable giving their phone to their partner or perhaps leaving it easily available, granting the partner easy access. Yet, even if a person guarded their phone with a passcode, the app can be downloaded remotely (Knibbs, 2015). Meaning, the user never has to touch the phone for the stalking to commence.

Apps such as mSpy feature three primary stalking services. In the case of domestic discord, for example, the abuser can listen in on a victim's phone calls, or choose to reject them entirely. The second feature, the keylogger option, allows the potential stalker to log every key a victim types, making reading their texts entirely possible. Lastly, the stalker can at any time, take

a video to know the victim's exact surroundings. Despite the overbearing presence of the app, the victim most likely will have no idea that they are being stalked.

When utilizing these features, the stalking potential becomes limitless. Similar to the dangers of spyware apps on a computer, identity theft is probable. However, when applied to romantic partners, the stalking can has the potential to become more invasive. A person using a spyware app can view photos, no matter how personal they may be. Even if they did not recognize their immediate surroundings through photo or video, those using the app have access to the GPS feature (Knibbs, 2015).

The GPS feature available in these apps is precisely what allowed a California man to find a woman's location at her friend's house, where he promptly murdered her in 2013 (Knibbs, 2015). Victims such as this woman may have been warned to turn off location services, but spyware apps are enduring; they cannot be turned off. Wherever the mobile device goes, the abuser can follow. The versatile cell phone, a communication medium once used to call the authorities to protect against stalking violence, has become the ultimate potential power tool for domestic abuse.

PREVALENCE AND USE

The intent to stalk domestic partners through spyware apps is rampant, but difficult to prove. Sadly, a myriad of victims have no idea that they are being stalked through their cell phones. Both mSpy and flexiSPY strongly imply that they are intended for stalking a cheating partner, through advertisement of recording phone calls and spying on texts (Knibbs, 2015). Even though 40% of spyware was downloaded with the intention to stalk a domestic partner even in 2002, it is difficult to prove these intentions through surveys (Calman, 2005). Those with a true intention to harm another person can easily lie to further protect their identity. Murky statistical data and support can be attributed to the prevalence of spyware apps as well as a lack of government regulation.

Murky Statistical Data and Support

MSpy and flexiSPY are incognito on the phones of those being abused (Shahani, 2014). The Department of Justice found that GPS technology and spyware monitoring affects 1 in 13 stalking victims (Fletcher & Kazdin, 2010). Knibbs estimates that spyware apps have received millions of downloads (2015). Therefore, comprehensive statistics on the prevalence of spyware app use are difficult to gather. Although mass media sources assure smartphone users that they

probably do not have to worry about spyware apps, domestic violence shelters illustrate a much different narrative. The recent rise of spyware app use has caused 85% of domestic abuse shelter advocates to have some experience with this form of abuse (Shahani, 2014).

As a result, precautions such as a "digital detox" have been taught to advocates in an attempt to cleanse the victim of all technology (Shahani, 2014). The private location of domestic violence shelters, digital detoxes, and advocates supporting victims all appear to remedy the tragedy that is reflected in the increasingly common use of cyberstalking. However, the obtrusive nature of these apps paired with GPS technology allows abusers to permeate through even supportive measures such as these (Knibbs, 2015). An abuser can always locate their victim with a spyware app, making the technology forever useful and ubiquitous.

Lack of Regulation

Fletcher & Kazdin tell the story of Susan*, a woman who experienced spyware stalking by an ex-boyfriend (2010). While enjoying dinner at a restaurant with a date, Susan would receive texts from her ex asking how the food was (Fletcher & Kazdin, 2010). GPS technology paired with the ability to read texts and listen on calls grants abusers the ability to know their ex-partner's every move. Although authorities put Susan's ex-boyfriend into custody, he showed up at her house twenty minutes after getting out of jail (Fletcher & Kazdin, 2010). Susan's story illustrates the lack of regulation in extreme cyberstalking cases. Unfortunately, the police cannot prove that spyware apps are illegal, as they are unregulated by the government. Apps like mSpy and flexiSPY defy wiretapping laws by technically marketing the apps towards employers and parents (Knibbs, 2015).

Hammad Akbar, creator of the spyware app StealthGenie was prosecuted for marketing illegal activity under the Wiretap Act (Knibbs, 2015). Akbar was only charged, however, because his website blatantly advertised the potential for abuse with his app. While certainly a victory for those affected by Akbar's abusive marketing ploy of technology, his prosecution was rare and perhaps an isolated incidence. Spyware has been pertinent since the late 1990's; the ability to stalk a partner has been relatively simple for years (Calman, 2005). Since the rise of spyware technology, only three prosecutions for the crime have been recorded (Knibbs, 2015). As long as apps like mSpy and flexiSPY are aware of legal loopholes, their creators will make adjustments to stay in big business.

LEGISLATION

Knibbs poses a noteworthy question after illustrating the dangers of spyware apps: how are these spyware apps not illegal? (Knibbs, 2015). Theoretically, the Wiretap Act that indicted Akbar should discourage other perpetrators from using these apps. The Wiretap Act prohibits any incognito interception of communication (Knibbs, 2015). Clearly, the acts of stalking and wiretapping are both recognized as illegal under the law. However spyware apps are entirely legal under federal law using this model, though the technology is designed to navigate technological and legal loopholes. When considering the grand scope of spyware apps, Hammad Akbar proves to be the exception of spyware app prosecution.

The outlook of spyware app use prosecution appears bleak, yet some believe legislation to ban the technology is in the foreseeable future (Dahl, 2014). Outreach from the Minnesota Coalition for Battered Women prompted Senator Al Franken to introduce *The Location Privacy Protection Act of 2014* (Franken, 2014). Franken's bill would end the development and usage of spyware apps—once and for all. In addition, the bill would require companies gathering personal data from smartphones to disclose what they were using the personal data for (Franken, 2014). Finally, authorities would be given precedent to prosecute individuals and seize their profits from spyware apps (Franken, 2014).

Franken's bill appears to be common sense. Nevertheless, his statistical data surrounding apps, anecdotal evidence of abuse from the local domestic violence shelter, and the strong support of Federal Trade Commission fail to convince consumers. The Software & Information Industry Association (SIIA) has expressed disdain for the bill, claiming it will stifle app innovation (Ramasastry, 2012). Citing the multi-stakeholder process, the SIIA argued that his bill obscures the initiative to boost user's preferences through data collection (Ramasastry, 2012). Four years of advocacy has not passed Franken's bill, despite its clear assistance to victims of domestic stalking. Because legislative efforts have been nominal, victim support centers remain the most pertinent resources for victims of domestic stalking.

METHODOLOGY

Three model universities with highly acclaimed programs for sexual assault survivors were e-mailed about their spyware app policies. The universities studied were influenced by the VAWA Task Force presentation by Shana Ware, Advocacy Services Coordinator at Northern Illinois University. Ware recognized universities that offered excellent advocacy services.

Representatives were contacted from Rutgers' Office for Violence Prevention and Victim Assistance, University of Michigan's Sexual Assault Prevention and Awareness Center, and University of New Hampshire's Sexual Harassment & Rape Prevention Program. In addition, representatives from Northern Illinois University's Health & Wellness Center, Advocacy Services, and the police department were interviewed to compare policies. Each representative was told that any response would be featured in my research. Despite a diverse outreach to different universities, the vast majority of persons contacted did not respond. Five respondents consented to interview. The responses were analyzed using thematic analysis.

In response to a lack of participation, I performed my own research given the university websites. In order to test the accessibility of the university's webpages, I used simple search terms that the average undergraduate student may use if effected. Using the keywords "stalking," "cyberstalking," and "spyware apps" I analyzed the resources available to students off of the university's main webpage.

RESULTS

I. INTERVIEWS

I utilized a thematic analysis from the little information I was given about spyware apps. Most individuals did not respond to my request, partially due to confidentiality issues. Yet, the information I was given was brief at best with three major themes most applicable.

Shifted or Shared Responsibility

Many individuals reported that they knew of the topic, but felt others had more formal way of discussing the apps. Namely, the police were cited as the most credible source when dealing with these apps. As one individual with information cited some useful information about the apps, they immediately referred me to the police as "they may have a more formal way of addressing the topic." These claims were not wrong, as the different victim support services and programs typically worked together when addressing spyware apps. A representative from University of Michigan told me, "[the] police department has a forensics technology division, and they assist survivors in doing forensics investigations of victim's computers and other electronic devices." Similarly, one respondent cited Title IX staff as an essential resource to assist Student Conduct. Even though victim support resources offered valuable resources, they were quick to share the responsibility with other departments to offer more comprehensive

support. Thus no entity other than police took responsibility for knowledge of spyware apps or their use.

Denial of Apps at Institution

Despite the scope and magnitude of spyware apps in domestic abuse shelters, some institutional respondents reported no spyware app usage on their campus. Three factors were offered as explanations within this theme, namely other types of stalking, no experience with spyware apps, or confidential content. Interestingly, one respondent stated that the small, inclusive nature of their campus did not require a student to use spyware to stalk; they most likely already knew the person's entire schedule. The respondent also noted social media served as a constant marker as to where the victim is at all times, noting, "spyware is not needed to find that person since the perpetrator already knows where to look."

Other participants noted that they "had no instances of spyware apps being used in stalking cases" but "[it] would [be] addressed only when it surfaces via audience members in presentations." Yet, a respondent from the same university explained that while they cannot recall an incident, "our investigation group is aware of them and there are too many to list." While awareness is pertinent, not all participants had the proper personal experience with the app to speak on the matter.

Current Practices

As for participants that had experience with spyware apps, some precautionary measures were noted. Police were always involved with the survivor support process, and forensics technology was used to detect the spyware. The efforts from the support programs coupled with the police resulted in prosecutions of those perpetuating domestic violence. In addition, advocates encouraged students to "regularly scan their computers for spyware or malware, change passwords frequently, and report suspicious activity." In other cases, advocates were aware of spyware apps, and offered hypothetical practices if they were presented with the technology. As one participant stated, "our office would follow the policies and procedures outlined in the Title IX policy and student code."

II. UNIVERSITY WEBSITE SEARCHES

The initial, and most accessible resource was the webpage of University of Michigan (https://www.umich.edu, April, 2016). When searching "stalking," the page featured 23,800,000 results. Particularly, the top results linked students to the notable Sexual Assault Prevention and

Awareness Center for support. Secondly, when examining "cyberstalking," the website featured 203,000 results. Multiple results included tips to block numbers on their mobile device and remove their social media presence. In addition, suggested resources were made for the victims on campus, off-campus, and with the police. Interestingly, despite the vast number of resources for stalking, the website featured only four results when examining, "spyware apps." The four results on spyware apps featured computer guidelines for traveling outside the university and coding lessons. One result examined privacy issues in Android applications. Yet, the privacy concerns centered around the government, and not on potential domestic abuse.

When examining the main Rutgers website, significantly less resources were featured in comparison to University of Michigan (http://www.rutgers.edu, April, 2016). "Stalking" produced 2,350 results. The Violence Prevention Program was featured first and foremost, as well as well as articles debunking myths that stalkers are not just "men in bushes." "Cyberstalking" produced significantly fewer results. Only 43 results were noted, a significant difference from the University of Michigan. Some information was made available on what cyberstalking is, a few vague unrelated academic journals were offered. Interestingly, there were 84 results for spyware apps. Yet, though these results warned of spyware and malware on computers, no information was offered on apps.

The final model university, University of New Hampshire had the least amount of resources (University of New Hampshire, 2016). The keyword "stalking" produced 1,200 results. The first few links connect students to the highly acclaimed Sexual Harassment and Rape Prevention Program (http://www.unh.edu, April, 2016). A sharp decline in results occurred when searching "cyberstalking," only yielding 33 results. Less information was linked to SHARPP. A Title IX report was featured as well. Primarily, cyberstalking produced students' presentations on what cyberstalking entails. Spyware Apps yielded 4 search results. There was little to no information actually regarding spyware apps, featuring only one student report on holiday scams from McAfee from 2013.

Lastly I compared the results to Northern Illinois University (Northern Illinois University, 2016). Although not chosen as one of the model universities, in no way does this comparison minimize the victim support efforts of Northern Illinois University. "Stalking" produced 361 results. Many of these links grant resources at the Women's Resource Center, Sexual Misconduct, and Advocacy Services. A diverse number of resource centers were listed

despite fewer results in general. Cyberstalking yielded only fourteen results. The Women's Resource Center proved to be most pertinent in defining cyberstalking and providing resources. However, these links are outdated as the Women's Resource Center has been renamed the Gender and Sexuality Resource Center. The Student Handbook also touches upon it. When examining "spyware apps," only six results are offered: two related to Nike's identity fraud, one to ResTech spyware on computers, and three to my own research, but offered only information about my politics. These resources do not offer information about the apps.

DISCUSSION

Limited interview data and few resources on university websites indicate that spyware apps remain largely unknown on college campuses. Advocates from some of the most well-known victim support centers appear to range from having no experience to moderate experience with these apps. The most experienced group proved to be law enforcement. The high frequency of cyberstalking experiences as well as a formulaic process for screening for spyware apps proves that the technology is a threat. The grave nature of spyware apps is heightened when victims have no idea that the apps even exist. Thus, it is necessary that awareness surrounding spyware apps be spread.

We must encourage advocates at domestic violence shelters, as well as university faculty & staff, and law enforcement to take the threat of spyware apps seriously. Apps like flexiSPY and mSpy are specifically designed to make a victim seem insane when reporting what their stalker knows. Like any form of stalking—in person or online, these threats must be acknowledged and properly addressed. Unlike cyberstalking on a computer, mobile apps hold the potential to be very powerful tracking devices for abusers. Therefore, proper protocol is necessary to not only shut down GPS location as some advocates noted, but to attack the problem at the root: preventative measures to dismantle the app entirely.

CONCLUSION

The lack of data on spyware apps is telling; even the most trained individuals may not know they exist. Clearly, the ubiquitous use of mobile technology on college campuses coupled with the naiveté of most young users should require both educational programming as well as technological instruction in the threat of spyware apps. Young people in particular typically have more experience with advanced technology. Additionally, the culture of college students sharing and partaking in technology use is conducive to spyware abuse. An abuser can find their next

stalking victim in a span of a minute if a willing student lends out their phone to a stranger, friend, or partner to make a phone call.

We cannot take the 'nomophobia' dependency of mobile devices lightly. An environment that normalizes constant mobile phone use will make spyware apps thrive. A consistent GPS location-tracking device only pinpoints the already constrained campus community, allowing an abuser to find their victim at an accelerated rate. This case study clearly indicates that the rapid change in technology is outstripping the changes in educational awareness and resources. It is essential that college campuses take this seriously and react both positively and assertively to educate their students about this potential threat.

The efforts of victim support units and police departments are to be applauded. When considering the novel nature of spyware apps, it is understandable that fewer resources exist. However, it is disconcerting that of the resources reviewed for this study, nominal information is provided to victims to combat the issue. Routine steps given to victims of cyberstalking, such as removing oneself from social media, turning off GPS locations, and changing their phone number, do not apply to this evolved form of technology. These apps hold the power to outsmart these meager efforts.

As attempts are made to debunk the "stranger in the bushes" myth of sexual assault, we must apply this reframed paradigm to stalking through spyware apps. Close friends and partners are most likely to have access to the victim's cell phone: not a complete stranger. A looming suspicion of cheating, an affordable payment, and a swift download make a person a victim to abuse without their knowledge. Legislative stagnation suggests that spyware apps are not going away anytime in the foreseeable future, thus support and education must be offered in the meantime. The research efforts and willingness to support these victims hold the potential for greater dialogue and policy changes in the future.

RESOURCES

Calman, C. (2005). Spy vs. Spouse: Regulating Surveillance Software on Shared Marital Computers. *Columbia Law Review*, 105(7), 2097-2134.

Campbell, J., & Moore, R. (2011). Self-perceptions of stalking victimization and impacts of victim reporting. *Police Practice and Research*, 12(6), 506-517.

Dahl, J. (2014, October 13). "Stalker apps" are legal, but maybe not for long. Retrieved from http://www.cbsnews.com/news/stalker-apps-are-legal-but-maybe-not-for-long/

Knibbs, K. (2015, January 30). How the Hell Are These Popular Spying Apps Not Illegal? Retrieved from http://gizmodo.com/how-the-hell-are-these-popular-spying-apps-not-illegal-1682660414

Northern Illinois University (2016). Retrieved April 08, 2016, from http://www.niu.edu/index.shtml

Ramasastry, A. (2012, December 18). Senator Franken Wants Us to Know When Our Apps Are Tracking Us: Why This Is a Sensible Thing for Congress to Require. Retrieved from https://verdict.justia.com/2012/12/18/senator-franken-wants-us-to-know-when-our-apps-are-tracking-us

Rutgers University (2016). Retrieved April 08, 2016, from http://www.rutgers.edu

Sen. Franken Reignites Efforts to End Stalking Apps Once and for All. (2014, March 27). Retrieved from https://www.franken.senate.gov/?p=press_release

Shahani, A. (2014, September 15). Smartphones Are Used To Stalk, Control Domestic Abuse Victimshani. Retrieved from http://www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims

Southworth, C.; Tucker, S. (2006-2007). Technology, Stalking and Domestic Violence Victims. *Mississippi Law Journal* 76(3), 667-676

Stalking Technology Outpaces State Laws. (2003). *Stalking Resource Center*, 3(2).

The Use of Technology to Stalk. (2012). Retrieved from https://victimsofcrime.org/our-programs/stalking-resource-center/stalking-information/the-use-of-technology-to-stalk

University of Michigan. (2016). Retrieved April 08, 2016, from https://www.umich.edu/

University of New Hampshire (2016). Retrieved April 08, 2016, from http://www.unh.edu

Wray, R. (2009, July 05). Nokia turns to Android in smartphone wars. Retrieved from http://www.theguardian.com/global/2009/jul/06/nokia-mobile-internet-phones