Cyberstalking Nature and Response Recommendations

Ioana Vasiu

Faculty of Law, Babeş-Bolyai University, Romania

Lucian Vasiu

Faculty of Law Cluj-Napoca, Dimitrie Cantemir University, Romania

Doi:10.5901/ajis.2013.v2n9p229

Abstract

Cyberstalking is a special form of stalking and involves the use of information and communication technologies as the means and the medium of harassment or intimidation. Cyberstalking can lead to significant and long lasting psychological, economic or even physical effects, and can be a platform for the commission of violent crimes. In the last decade, cyberstalking has received significant attention from researchers, lawmakers, policy officials, and law enforcement agencies. Yet, although there is a significant body of literature on the topic, which recognizes cyberstalking as a very serious and growing problem and discusses various aspects of it, we believe that the phenomenon is not sufficiently examined, particularly considering the rapidly evolving technologies, which give perpetrators unprecedented capabilities. In this paper, in an interdisciplinary approach, we review relevant research and look into the criminalization of cyberstalking. Our paper extends existing knowledge of the phenomenon by analyzing a number of recent real cases, obtained mainly through an online legal research service, to reveal the nature of cyberstalking. We outline the most important aspects and issues raised by this phenomenon and make a number of recommendations as possible solutions to mitigating the risk, from education and awareness to adequate technology and legal response.

Keywords: *Cyberstalking, Cyberharassing, Information and Communication Technologies, Malware, False personation.*

1. Introduction

Cyberstalking is a specialized form of stalking (Reyns, 2010) and involves the use of information and communication technologies as the means and the medium of harassment or intimidation. Cyberstalking represents a violation of several fundamental human rights, such as the right to life, liberty and security, and can represent a very serious interference with the victim's privacy, family or correspondence. In recent years, due to a number of high profile cases, some ending tragically for victims, cyberstalking has received significant attention from policy makers and researchers (Huffman & Overton, 2013; Reyns et al., 2012; Rowan, 2012; Reyns et al., 2011; Lipton, 2011; Wang & Kraft, 2010; Baer, 2010; Salter & Bryden, 2009; Sheridana & Granta, 2007; Pittaro, 2007; Goodno, 2007; Petrocelli, 2005; Spence-Diehl, 2003; D'Ovidio & Doyle, 2003; Spitzberg & Hoobler, 2002; Ellison & Akdeniz, 1998).

There is no generally accepted definition of cyberstalking; moreover, as Lipton (2011) observes, there is significant overlapping between 'cyberstalking', 'cyber-harassment' and 'cyber-bullying'. In general, 'stalking' is defined as persistently or obsessively harassing someone in ways that alarm, torment, intimidate or frighten them. Some legal commentators, such as Ajmani (2011) or Parsons-Pollarda & Moriarty (2009), believe that cyberstalking is a new form of stalking. According to the definition proposed by Bocij and L. McFarlane (2002), cyberstalking is a group of behaviors in which an individual, group of individuals or organization uses information and communication technologies to harass one or more individuals; such behavior may include, without being limited to, the transmission of threats and false accusations, identity theft, data theft, damage to data or equipment, computer monitoring and the solicitation of minors for sexual purposes. In some cases, the illegal behavior can span a very long time, more than three decades in one case (e.g., *U.S. v. Shrader*).

According to Baum et al. (2009), roughly 1 in 4 stalking victims reported some form of cyberstalking, such as e-mail (83%) or instant messaging (35%), while electronic monitoring and Global Positioning System (GPS) technology were used in a number of cases. The criminal phenomenon of cyberstalking is difficult to quantify; as King-Ries (2011) remarks, data on cyberstalking is still in its infancy. As cyberstalking can have a very negative impact on victims, resulting in anxiety or fear and loss of trust in people, it needs to be effectively addressed by stakeholders.

There is a significant body of literature on cyberstalking, which discusses various aspects of the phenomenon, including several classifications. According to Brenner (2010), there are four categories of cyberstalkers: the ex-partner, the romantic fantasist, the dangerous obsessed, and the sadist. McFarlane & Bocij (2005) propose a classification that contains the following types of stalkers: composed, intimate, collective and vindictive. However, in accord with Nobles et al. (2012) and Parsons-Pollarda & Moriarty (2009), we believe that the nature of the phenomenon is not sufficiently known, that more research in the field is needed, particularly considering rapidly evolving technologies, such as malware, social media, geotagging and geocoding, which give perpetrators unprecedented capabilities.

In this paper, we address this need for an in-depth examination of the nature of cyberstalking. To that end, we studied over one hundred real cases brought before courts, the vast majority obtained through an online legal research service. We also studied releases from the U.S. Department of Justice (USDoJ) and articles published on news sites. We report the most relevant cases with respect to perpetrator's profile, relation with victim, and course of conduct involved.

The rest of this paper is organized as follows: in the next section, we look into the criminalization of cyberstalking in several jurisdictions. Next, based on the cases studied, we outline the nature of cyberstalking. Finally, we draw our conclusion, which includes a number of response recommendations.

2. Criminalization of cyberstalking

Although a relatively new criminal phenomenon, cyberstalking is criminalized in virtually all U.S. and E.U. states. In the U.S., a person can be found guilty of cyberstalking under 18 U.S.C. § 2261A: the perpetrator must act "with the intent to kill, injure, harass, or intimidate another person", and, in doing so, places the victim in reasonable fear of death of, serious bodily injury to, or causes substantial emotional distress to that person; a person may also be found liable if reasonable fear of death, serious bodily injury, or emotional distress happens to a person's immediate family member, spouse, or intimate partner. There are recent legislative bills that aim to better address the issues raised by cyberstalking and help law enforcement to more effectively target the perpetrators.

Several U.S. states have enacted cyberstalking laws that explicitly include electronic forms of communication within more traditional stalking laws. These laws, however, are not uniform, varying in terms of conduct criminalized, standards that would trigger prosecution, penalties, and/or protection offered for victims. California was the first state in the U.S. that criminalized cyberstalking: according to California Penal Code (Section 646.9), "Any person who willfully, maliciously, and repeatedly follows or willfully and maliciously harasses another person and who makes a credible threat with the intent to place that person in reasonable fear for his or her safety, or the safety of his or her immediate family is guilty of the crime of stalking" ("credible threat" is defined as "a verbal or written threat, including that performed through the use of an electronic communication device"). According to California Civil Code § 1708.7, "a person is liable for the tort of stalking when the plaintiff proves all of the following elements of the tort: (1) the defendant engaged in a pattern of conduct the intent of which was to follow, alarm, or harass the plaintiff" and "(2) as a result of that pattern of conduct, the plaintiff reasonably feared for his or her safety, or the safety of an immediate family member". In the state of Florida (784.048), cyberstalking is defined as "means to engage in a course of conduct to communicate, or to cause to be communicated, words, images, or language by or through the use of e-mail or electronic communication, directed at a specific person, causing substantial emotional distress to that person and serving no legitimate purpose". In the state of Louisiana (§40.3), cyberstalking is defined as the action of any person to accomplish any of the following: "(1) Use in electronic mail or electronic communication of any words or language threatening to inflict bodily harm to any person or to such person's child, sibling, spouse, or dependent, or physical injury to the property of any person, or for the purpose of extorting money or other things of value from any person; (2) Electronically mail or electronically communicate to another repeatedly, whether or not conversation ensues, for the purpose of threatening, terrifying, or harassing any person; (3) Electronically mail or electronically communicate to another and to knowingly make any false statement concerning death, injury, illness, disfigurement, indecent conduct, or criminal conduct of the person electronically mailed or of any member of the person's family or household with the intent to threaten, terrify, or harass; (4) knowingly permit an electronic communication device under the person's control to be used for the taking of an action in paragraph (1), (2), or (3)".

In the E.U., there is no consensus as to the definition of cyberstalking (Modena Group on Stalking, 2007). Underlining the dangers presented by this criminal phenomenon, one recent document calls on the European Commission to have the crime of stalking/cyberstalking included in the new Criminal Justice Bill for the European Union amendment for Victims' Rights (European Commission, 2010).

3. Nature of cyberstalking

The cases we studied show that cyberstalkers present virtually no restriction with respect to age, gender, marital status, sexual orientation, and ethnic, cultural, economic or intellectual background. In one case, a 12-year old girl was convicted of cyberstalking (Myers, 2011). In some cases, perpetrators knew the victim, while in other cases found the victim through search engines, online forums or social networks (such as MySpace, Facebook, Friendster, Twitter etc.). In a number of cases, cyberstalking involved spouses that broke up (e.g., *People v. Rosa* and *U.S. v. Walker*). In some cases, after the romantic relationship has ended, women engage in cyberstalking (e.g., *Vrasic v. Leibel),* while in other cases the perpetrator was seeking a romantic or sexual relationship, victims being, often, a celebrity, such as an actress (*U.S. v. Gagnon*) or a model (Miles, 2012; Schram & Amos, 2012). The victims of cyberstalking are mostly women, of virtually any age or ethnicity. Cyberstalking has various motivations, from revenge and hate, to erotic obsessions. A number of perpetrators suffered from bipolar disorder (e.g., *U.S. v. Juliano* or *U.S. v. Stacy*) or schizophrenia (e.g., *U.S. v. Gagnon*).

We found that perpetrators met their victims in a large number of settings. For instance, in *State v. Gandhi*, defendant initially met the victim through a mutual friend. In *U.S. v. Infante*, the defendant met the victim at University. In *People v. Chase*, the perpetrator and the victim were next-door neighbors. In *People v. Casarez*, perpetrator met the victim at work. In one case (USDoJ, 2010), victims were customers of an online store that operated a fraudulent scheme by selling counterfeit and inferior quality goods and making unauthorized charges: when victims complained, they were cyberstalked through a campaign of aggressive, obscene, and intimidating conduct. In *People v. James*, perpetrator and victim became acquainted while attending a vocational program.

In some cases, perpetrators did not know the victim previously. In *People v. Costales*, victim used an "an open profile" MySpace account to market her music; she received a large number of disturbing e-mails from a Michigan person, a stranger for her. In *People v. Corleone*, perpetrator met the victim via an advertisement for "adult services", posted on the Craigslist website. In *U.S. v. Crisman*, perpetrator stole customer information at Best Buy to cyberstalk the customers he found attractive.

With respect to the course of conduct, we noted that electronic communications and creation of fake websites or advertisements are very often used by perpetrators. In *People v. Corleone*, perpetrator created a webpage on MySpace and portrayed the victim as a prostitute, whose mother was her "pimp". In *U.S. v. Sayer*, perpetrator created a fake Facebook account for a former girlfriend, fictitious Internet advertisements and social media profiles using victim's name, the fictitious Internet postings including victim's address and an invitation to visit her for sexual encounters. In *People v. Rosa*, false personation was involved, perpetrator placing on a website photographs of his former wife in the nude and advertisements that the victim was keen to meet men for oral sex. In *Vrasic v. Leibel*, the perpetrator sent offensive letters and a naked photograph of victim to those on his contact list and created a website on victim's name to pre-sell her book and to post an excerpt that included defamatory statements about him.

In *State v. Gandhi*, the course of conduct consisted of sexually graphic and threatening e-mails, which contained the details of defendant's desire to have sex with the victim. In *U.S. v. Grob*, after the couple broke up, perpetrator sent his ex-girlfriend a large number of threatening e-mails and text messages (e.g., "I'm going to slit your throat"), some messages having attached photographs of dead and dismembered women. In *U.S. v. Bowker*, perpetrator sent several e-mails with attached photographs with verbal captions, one caption referred to the victim as being shot with a pellet gun. In *U.S. v. Petrovic*, during the relationship with the perpetrator, victim occasionally allowed the taking of pictures of her in the nude and while performing various sexual acts, and confided in the perpetrator, revealing intimate or personal information in text messages (such as the sexual abuse suffered as a young girl, suicidal thoughts, and family secrets), all subsequently posted by the perpetrator on a website, who also sent photographs of victim engaging in sex acts to various people, from victim's boss to her family members. In *State v. Hemmingway*, perpetrator's e-mail and text communications with his ex-wife threatened her ("I have not killed anyone in a long time. I don't know who's going to be first, you or me"). In *U.S. v. Walker*, as part of the battle for child custody, the perpetrator forced his child to send e-mails composed by him, containing derogatory words, such as "whore" or "bitch", and threats to harm the victim, to his former wife. In *U.S. v. Juliano*, defendant sent threatening e-mails, causing substantial emotional distress to the recipient and placing the victim in reasonable fear of serious bodily injury. In *People v. Casarez*, e-mail and text messages were used to insult and scare the victim ("How is my dirty little whore" and "did I mention I tested HIV positive?"). In *People v. Chase*, perpetrator sent threatening e-mails to the victim ("there will be hell to pay").

In a trans-border case reported by The Economist (2011), the perpetrator sent to a mezzo-soprano about 4000 Internet messages over a period of five years, depicting the victim as a talentless, sex-crazed swindler. Internet and text messages were used by Allen (USDoJ, 2012) to communicate with a number of female victims, telling them that he found naked pictures of them on the Internet and threatened victims that, unless they take their clothes off and engage in sexual

conduct, those naked pictures would be released online. In *State v. Nahimana*, perpetrator sent communications from his MySpace account to the victim's account. Campbell (USDoJ, 2011a) stole a number of private photographs and videos that were stored on victims' computers and posted the stolen files on various websites, to harass and cause emotional distress to victims.

Electronic surveillance is increasingly used by cyberstalkers: for instance, the use of malware, such as the use of RemoteSpy to spy on victims (*Federal Trade Commission v. Cyberspy Software*, *LLC*) or of keylogger programs to observe victims' Internet usage (USDoJ, 2011), or the use of Global Positioning System technology, to track the location or movement of victims (*U.S. v. Curley*).

4. Conclusion

Cyberspace presents numerous opportunities for cyberstalkers. Cyberstalking has become a very real problem in today's world, one that can have devastating consequences for victims, especially in cases of obsession or derangement. Virtually everybody can become the victim of cyberstalking. Perpetrator's conduct can include annoying or threatening e-mails (including threats of rape and physical violence or lustful, obscene or vulgar words), malicious comments on websites or false website ads, illegal access to victim's e-mail account, impersonation in chat rooms, creation of webpages pages under victim's name, publication of Twitter posts, posting of nude photos or lewd videos on Facebook, use of malware etc.

During our research, we found an alarming number of cyberstalking cases, many inflicting significant emotional distress or mental anguish on victims. Due to several characteristics of the online environment, such as perceived anonymity, easiness in meeting and contacting victims, and reduced chances of apprehension, we can only expect that cyberstalking will become increasingly prevalent. It is important that educational programs address these online risks and the various methods employed by perpetrators, so that potential victims would limit the opportunities available to cyberstalkers. It is also important that users protect their online privacy and secure their computer data, use technology to block out unwanted messages, use improved identity management technology, and learn how to preserve the evidence of the illegal conduct.

There is a clear need for a streamlined procedure for the take-down of webpages in situations of false personation. There is also a need for an improved legal framework, to effectively address this criminal phenomenon, which we consider under-prosecuted, including tougher punishment for such crimes. Moreover, as cyberstalking is an international criminal phenomenon, we believe that it must be included in the Convention of Cybercrime and in a future global Cyber Treaty, to allow cooperation in the gathering and sharing of evidence, and in the bringing of perpetrators to justice.

References

Ajmani, N. (2011). Cyberstalking and Free Speech: Rethinking the Rangel Standard in the Age of the Internet. Oregon Law Review, 90, 303-333.

Baer, M. (2010). Cyberstalking and the Internet Landscape We Have Constructed. Virginia Journal of Law & Technology, 15(154), 154-172.

Baum, K., Catalano, S., Rand, M. & Ros, K.. (2009). USDoJ, Bureau of Justice Statistics, Special Report January 2009.

Bocij, P. & McFarlane, L. (2002) Online harassment: Towards a definition of cyberstalking. Prison Service Journal, 139, 31-38.

Brenner, S.W. (2010). Cybercrime: Criminal Threats from Cyberspace. Praeger.

D'Ovidio, R. & Doyle, J. (2003). A study on cyberstalking: Understanding investigative hurdles. FBI Law Enforcement Bulletin, 72(3), 10-17.

European Commission (2010). Application for stalking to be included in the new Criminal Justice Bill for the European Union. Retrieved from: http://ec.europa.eu/justice/news/consulting_public/0053/contributions/organisations/Unregistered/net_for_surviving_stalking_en.pdf.

Ellison, L. & Akdeniz, Y. (1998). Cyber-stalking: the Regulation of Harassment on the Internet, Criminal Law Review, December Special Edition, 29-48.

Goodno, H. N. (2007). Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws. Missouri Law Review, 72, 125-196.

Huffman, J. & Overton, A. (2013). Missing the Mark: The Neglect of Stalking and Cyberstalking in Introductory Criminology Textbooks. Journal of Criminal Justice Education, 24(2), 200-217.

King-Ries, A. (2011) Teens, Technology, and Cyberstalking: The Domestic Violence Wave of the Future?. Texas Journal of Women and the Law, 20 (2), 131-164.

Lipton, J. (2011). Combating Cyber-victimization. Berkeley Technology Law Journal, 26, 1104-1155.

McFarlane, L. & Bocij, P. (2005). An exploration of predatory behaviour in cyberspace: Towards a typology of cyber stalkers. First Monday, 8.
Miles, K. (2012). LA Model, Facebook Stalked By Man Threatening To Kill Her, Retrieved from: http://www.huffingtonpost.com/2012/06/28/kourtney-reppert-la-model-facebook-stalked_n_1634557.html.
Modena Group on Stalking (2007). Protecting Women from the New Crime of Stalking. A Comparison of Legislative Approaches within the European Union, Final Report, University of Modena and Reggio Emilia for the European Commission.
Myers, L. (2011) Girl, 12, gets probation in cyber-stalking case, Retrieved from: http://www.reuters.com/article/2011/07/13/us-crime-girl-cyberstalking-idUSTRE76C74C20110713.
Nobles, M.R., Reyns, B.W., Fox, K.A. & Fisher, B.S. (2012). Protection Against Pursuit: A Conceptual and Empirical Comparison of Cyberstalking and Stalking Victimization Among a National Sample. Justice Quarterly.
Parsons-Pollarda, N. & Moriarty, L.J. (2009). Cyberstalking: Utilizing What We do Know. Victims & Offenders: An International Journal of Evidence-based Research, Policy, and Practice, 4(4), 435-441.
Petrocelli, J. (2005). Cyber stalking. Law & Order, 53(12), 56-58.
Pittaro, M. L. (2007). Cyber stalking: An Analysis of Online Harassment and Intimidation. International Journal of Cyber Criminology, 1(2), 180–197.
Reyns, B.W. (2010). A situational crime prevention approach to cyberstalking victimization: Preventive tactics for Internet users and online place managers. Crime Prevention and Community Safety, 12, 99–118
Reyns, B.W., Henson, B. & Fisher, B. S. (2011) Being Pursued Online: Applying Cyberlifestyle–Routine Activities Theory to Cyberstalking Victimization. Criminal Justice and Behavior November, 38, 1149-1169.
Reyns, B.W., Henson, B., Fisher, B.S. (2012). Stalking in the Twilight Zone: Extent of Cyberstalking Victimization and Offending Among College Students. Deviant Behavior, 33(1), 1-25.
Rowan, M. (2012). When words hurt more than "sticks and stones": why New York state needs cyberbullying legislation. Albany Law Journal of Science and Technology, 22(3), 645-674.
Salter, M. & Bryden, C. (2009). I can see you: harassment and stalking on the Internet. Information & Communications Technology Law, 18(2), 99-122.
Schram, J. & Amos, C. (2012). SI model nails cyber-stalker accused of uploading her photos onto a porn site, Retrieved from: http://www.nypost.com/p/news/local/staten_island/si_model_this_is_bust_QPWIht8gmuGkbe2jzI5i6K.
Sheridana, L.P. & Granta, T. (2007). Is cyberstalking different?. Psychology, Crime & Law, 13 (6), 627-640.
Spence-Diehl, E. (2003). Stalking and technology: The double-edged sword. Journal of Technology in Human Services, 22(1), 5-18.
Spitzberg, B. H. & Hoobler, G. (2002). Cyberstalking and the technologies of interpersonal terrorism. New Media & Society, 4(1), 67–88.
The Economist (2011). Creepy crawlies, Retrieved from: http://www.economist.com/node/18584386.
USDoJ (2011). Retrieved from: http://www.justice.gov/usao/cas/press/cas11-0608-Lutz.pdf.
USDoJ (2012). Michigan man charged with cyberstalking and attempted sexual exploitation of minor victims. Retrieved from: http://www.justice.gov/usao/nyw/press/press_releases/Allen3.pdf.
USDoJ (2011a). Computer hacker pleads guilty to cyberstalking and unauthorized access to a computer. Retrieved from: http://www.justice.gov/usao/flm/press/2011/july/20110720_Campbell_Tpa_PSCArrestplea.pdf.
USDoJ (2010). Manhattan U.S. attorney charges operator of luxury eyewear website with cyberstalking, threatening, and defrauding his customers. Retrieved from: http://www.justice.gov/usao/nys/pressreleases/December10/borkervitalyarrestpr.pdf.
Wang, J. & Kraft, E. (2010). An Exploratory Study of the Cyberbullying and Cyberstalking Experiences and Factors Related to Victimization of Students at a Public Liberal Arts College. International Journal of Technoethics, 1(4), 74-91.

List of cases

Federal Trade Commission v. Cyberspy Software, Llc, No. 6:08-cv-1872-Orl-31GJK (United States District Court, M.D. Florida, Orlando Division, 2009).
People v. Casarez, Nos. A123927, A126667 (Court of Appeals of California, First District, Division Three, 2010).
People v. Chase, No. 09CA1908 (Court of Appeals of Colorado, Division VI, 2013).
People v. Corleone, D052816 (Court of Appeals of California, Fourth Appellate District, Division One, 2009).
People v. Costales, 2d Crim. No. B215915 (Court of Appeals of California, Second District, Division Six, 2010).
People v. James, Nos. A124954, A126576 (Court of Appeals of California, First District, Division One, 2010).
People v. Rosa, No. F063748 (Court of Appeals of California, Fifth District, 2013).
State v. Gandhi, 989 A.2d 256 (2010).
State v. Hemmingway, 825 N.W.2d 303 (2012).
State v. Nahimana, 285 P.3d 763 (2012).
U.S. v. Bowker, No. 4:01CR441 (United States District Court, N.D. Ohio, Eastern Division, 2010).
U.S. v. Crisman, No. CR 11-2281 JB (United States District Court, D. New Mexico, 2011).
U.S. v. Curley, 639 F.3d 50 (2011).
U.S. v. Gagnon, No. 08-8230 (United States Court of Appeals, Fourth Circuit, 2009).
U.S. v. Grob, 625 F.3d 1209 (2010).
U.S. v. Infante, 782 F.Supp.2d 815 (2010).

U.S. v. Juliano, No. 10-234 (United States District Court, W.D. Pennsylvania, 2011).
U.S. v. Petrovic, 701 F.3d 849 (2012).
U.S. v. Sayer, No. 2:11-CR-113-DBH (United States District Court, D. Maine, 2012).
U.S. v. Shrader, 675 F.3d 300 (2012).
U.S. v. Stacy, No. CR 11-1878 JB (United States District Court, D. New Mexico, 2013).
U.S. v. Walker, 665 F.3d 212 (2011).
Vrasic v. Leibel, No. 4D12-1289 (District Court of Appeal of Florida, Fourth District, 2013).