The Use of Technology to Stalk and the Workplace

By Maya Raghu[1]

"Mary" met Kenneth Kuban, an employee of the Library of Congress, on a dating website in 2010. Mary ended in the relationship in April 2011, but received numerous daily phone calls and emails from Kuban for four months, asking her to reconsider. Mary obtained a restraining order in July 2011. According to an indictment, Kuban then impersonated Mary and posted ads on Craigslist soliciting sexual encounters. As a result, for over three months strangers from all over the country came to Mary's home seeking sex.

Mary reported Kuban's actions to his employer, the Library of Congress. Pursuant to an investigation, federal agencies and law enforcement determined that Kuban was posting the online sex ads during work time from an IP address at the Library of Congress, and that his email was used to post the ads on Craigslist. Kuban was arrested and charged with stalking, identification fraud and other crimes.[2]

This incident illustrates behavior that is disturbing and criminal – but sadly, not unusual. It occurs much more frequently than reports and statistics indicate, and it happens quite often in the workplace. Today many people spend a substantial amount of time at work, and use work-provided computers, smartphones and internet access to conduct personal matters. When employees engage in harassing or threatening behavior or stalking on work time with work resources, it becomes an employer's business.

What is Stalking and How Does Technology Play a Role?

Stalking is generally a course of conduct directed at a specific person that would cause a reasonable person to feel fear. Stalking behavior includes, but is not limited to: following or spying on a person, waiting at places in order to make unwanted contact with the victim or to monitor the victim, leaving unwanted items and gifts for the victim, and posting information or spreading rumors about the victim on the internet, in a public place, or by word of mouth. Stalking is strongly correlated to sexual assault and domestic violence. Approximately 1 in 6 women (16.2%) and 1 in 19 men (5.2%) in the United States have been victims of stalking.[3] Nearly three out of four stalking victims knew his or her offender in some capacity and 21.5% of stalking victims identified their stalker as a former intimate.[4]

Over the last 15 years, the incidence of stalking through the use of technology (or "cyberstalking" as it is commonly known) has sharply increased. The term refers to the use of the internet, email, or other telecommunication/electronic technologies to harass or stalk another

[1] Special thanks to staff at the Stalking Resource Center, a partner in the project Workplaces Respond to Domestic and Sexual Violence: A National Resource Center, for their assistance with this article.

[2] Justin Jouvenal, "Stalkers Use Online Sex Ads as Weapon," *The Washington Post*, July 14, 2013.

[3] Centers for Disease Control, National Center for Injury Prevention and Control. *The National Intimate Partner and Sexual Violence Survey (NISVS): 2010 Summary Report* (2011).

[4] U.S. Department of Justice, *National Crime Victimization Study* (2005); Katrina Baum, *Stalking Victimization in the United States*, U.S. Department of Justice, Bureau of Justice Statistics (2009).

person.[5] Perpetrators can use technology by itself to stalk a victim, or in conjunction with an ongoing pattern of conventional stalking. A recent study by the U.S. Department of Justice found that the top two forms of stalking behaviors experienced by victims were unwanted phone calls and messages (66.7% of victims surveyed) and unwanted letters and email (30.7% of victims surveyed).[6] Other examples of technology used to stalk include:

- Email spoofing, whereby the perpetrator sends emails pretending to be the victim
- Text messaging and sexting (sending sexually explicit text messages and/or photos)
- Social media (Facebook, Twitter, Instagram, etc.); creating social media accounts to harass, threaten and/or denigrate the victim[7]; impersonating the victim on social media
- Online impersonation of the victim through a false identity or account to place online sex ads or solicit sex
- Use of GPS to track the victim, including placing a GPS device on the victim's car.

Legal Context

Stalking is a crime under federal law[8] and the laws of 50 states, the District of Columbia, the U.S. Territories, and many Indian Tribes. In addition to stalking, every jurisdiction in the U.S. has laws addressing electronic harassment, and federal law also criminalizes the use of technology to stalk.[9] Legal definitions of stalking and harassment vary from one jurisdiction to another, especially with regard to the perpetrator's intent, the victim's fear or emotional distress, and the level of fear experienced by the victim.[10]

In recent years a handful of states also have passed laws criminalizing impersonation of individuals on the internet, including New York, California and Texas. In New York and California, online impersonation is a misdemeanor punishable by fines and up to a year in prison. In Texas, the crime is a felony punishable by up to ten years in prison.[11]

---

[5] *See* Trudy M. Gregorie, "Cyberstalking: Dangers on the Information Highway." National Center for Victims of Crime (2001).

[6] Shannan Catalano, *Special Report: Stalking Victims in the United States – Revised*, at 4. U.S. Department of Justice, Bureau of Justice Statistics (September 2012).

[7] For example, a person created multiple Twitter accounts to harass a Philadelphia talk radio host for an on-air remark. "Fox 29 Explores Cyberstalking," July 24, 2013, available at http://www.myfoxphilly.com/story/22926663/fox-29-explores-cyber-stalking.

[8] Interstate stalking, which is frequently an aspect of domestic or intimate partner violence, is a federal crime. *See* 18 U.S.C. §2261A.

[9] 18 U.S.C. §2261A criminalizes using "any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate or foreign commerce" that places a person in reasonable fear of death or serious bodily injury or substantial emotional distress.

[10] To learn how each state's law defines stalking, see the website of our project partner, the Stalking Resource Center, http://www.victimsofcrime.org/our-programs/stalking-resource-center/stalking-laws.

[11] *See* Cal. Pen. Code § 528.5; N.Y. Pen. Law §190.25; Tex. Pen. Code § 33.07.

Despite these new laws, specialists and victim service providers observe that technology is rapidly outpacing the boundaries of the law and surpassing law enforcement's ability to identify, investigate and prosecute technology-enabled stalking.[12]

What Can Employers Do to Address the Workplace Implications?

Technology-enabled stalking and harassment become workplace issues in two major ways: when an employee is the victim of such acts, and when an employee is the perpetrator. Because the harassment and/or or stalking occurs while the victim- or perpetrator-employee is at work, and may involve the use of work resources -- an employer-provided computer, smartphone, telephone, and internet access -- it becomes the employer's concern; employers have a duty to provide a safe workplace and to address an employee's potentially criminal behavior.

The best approach is for employers to get ahead of the issue, and not wait to react to a particular incident. Employers should strive to create a healthy and safe work environment free of harassment and stalking, by instituting both preventative and remedial measures. Employers should make clear that harassing, threatening or stalking behavior is not acceptable inside or outside of the workplace, and will be addressed. If an employee complains of harassment or stalking via technology while at work, an employer should not dismiss their concerns or simply refer them to EAP. Similarly, if someone reports an employee for harassing or stalking them using technology, the best practice is for employers to take the complaint seriously and initiate an investigation. The actions of the Library of Congress employee, Kenneth Kuban, demonstrate how employees can use work time and technology to perpetrate stalking and harassment that is not immediately obvious. Employers should document all reported instances of harassment by the employee-perpetrator and seek the assistance of law enforcement (after consulting the victim).

Another important piece of a healthy and safe work environment is to address the use of workplace technology. The best and most comprehensive way to address this is through a technology policy. Employers should clearly set forth the organization's appropriate and acceptable uses for the employer-provided telephone, smartphone, computer, and internet access. Employers also should take steps to prevent employee identity theft through the use of technology, especially through work-provided devices. Issues to consider and address include:

- Are all work-provided devices and accounts password-protected?
- Is personal employee or client information that is stored in company databases or on servers electronically encrypted?
- Can employees use work resources to access non-work related content during work hours, or during personal time?
- Are employees allowed to access personal email or social media (Facebook, Twitter, etc.) from work devices?

[12] *See* Stalking Resource Center, "Stalking Technology Outpaces State Laws," available at http://www.victimsofcrime.org/docs/src/stalking-technology-outpaces-state-laws17A308005D0C.pdf?sfvrsn=2.

- Does the employer monitor, prevent access to or block objectionable content and/or websites?

The policy should clearly set forth the procedure to be followed if an employee violates the policy, uses work-provided technology to harass, threaten or stalk, and the potential consequences.

Addressing workplace safety is a vital part of a comprehensive workplace violence program. For more information, see the Workplaces Respond website and the Stalking Resource Center's website.

Maya Raghu is a senior attorney at Futures Without Violence, a non-profit organization and lead partner in Workplaces Respond to Domestic and Sexual Violence: A National Resource Center.