Brendan Marcelo
CYSE201S
Article #2

Intimate threats: The most common yet overlooked vulnerability

Through a social science lens, privacy threats in intimate relationships examine the relationship between technology and human behavior. This study shows how the threats and vulnerabilities of intimate relationships are treated as routine and often overlooked, but they are experienced more frequently. Intimate threats threaten valuable and personal data like financial records, photographs, login/passwords, and privacy rights. These threats can be the first step to financial fraud and physical, emotional, and sexual abuse. The article explains its importance in the social structures and cultures of relationships between significant others, parents and their adolescent children, and adults/young adults who are caretakers of their parents.

Relativism states that all things are related. Through a systems perspective, changes in one system led to changes in another system. In cybersecurity - social systems change are driven by technology. This article demonstrates how changes in technology can have a significant influence on social behavior. For example, according to studies in the article it is very common for significant others to share private information with each other due to shared accounts, cell phone plans, and by simply living in the same household. When an individual notices changes in attitude or sneaky behavior in their partner, they are more subject to hack into their accounts to view their messages, social media platforms, and even bank statements.

The behavioral theory suggests that behavior is learned. The sources of learning include family, schools, mass media, and environmental influences. This theory relates to privacy in intimate relationships by concentrating on the effect of behaviors in relationships due to situational dynamics and learned patterns of one another. The behavioral theory hypothesizes that actions are caused by consequences. Monitoring behaviors tend to seek the reward of safety, control, and trust. Parents and significant partners may track each other or monitor each other through GPS tacking apps to ensure safety and maintaining trust. Situational dynamics also lead to privacy violations. Couples who share accounts, back up devices, or family plans are more subject to unintentionally share passwords, security questions, and other private information. The

emotional trigger of jealousy or fear is an influence of controlling a significant others digital presence. This theory is also responsible for how these behaviors are more common over time. Although there are many privacy rights violated, monitoring is acceptable with keeping an eye on elderly relatives and supervision over children.

According to module 8, the American sociological association defines sociology as "the study of social life, social change, and the social causes and consequences of human behavior." This is relevant to the privacy threats within intimate relationships because threats arise from dynamics in relationships from families to romantic partnerships. Within families, sociology studies family dynamics and their influence on behavior. Parents and intimate partners ensure safety and trust by monitoring or sharing passwords. Sociology raises awareness to where monitoring and sharing private information can be a caring behavior, but it can easily shift into an abusive behavior and an invasion of privacy. We can use sociology to investigate negative effects of individuals actions. The article highlights how privacy violations are more commonly seen in women, children, and the elderly. For example, abusive partners use monitoring tools such as spyware to harm or control their victims eventually leading to physical abuse. A social investigation would associate patterns of this behavioral pattern to gender equality

The different types of research done in this article, classifies the four different groups in which intimate attacks happen: intimate partners, parents and minor children, adult children and elderly parents, and friends. Privacy threats emerge often in romantic partnerships from casual to abusive over the course of their relationship. Nearly 1 in 3 women and 1 in 6 men experience abuse over the course of their relationship (Levy & Schneier, 2020). An increasing number of these cases utilize technology to abuse and control their victim. They consist of off the shelf spyware apps which are readily available for download on app stores. These apps run in the background on the victim's phones, tablets, or laptops reporting their activities to the abuser. Smart home technologies like web-enabled cameras, home appliances, and other home sensors are used to stalk, harass, and monitor their victims' activities. Researchers evidence showed 40 academic analyses of smart home security anticipated 29 different threat actors and 100 different types of threats, while the threat of physical/domestic abuser was almost entirely absent. According to the article, there is a company that markets a mattress that detects and reports suspicious movements in the bed. NPR survey of US domestic violence shelters indicated that 85% of shelters had worked with survivors who had been victims of abuse through

eavesdropping tools and surveillance devices. Abusers also rely on the ease of access of the victim's personal information like passwords, answers to their security questions, and other authentication mechanisms to help gain more access to their information.

Parents are known to monitor their children for safety reasons from infancy to young adult hood. A Pew survey found that the majority of parents check their teenagers browsing histories, texts, and social media profiles. 16% tracked teens' locations via their cell phones – half reported knowing the password to their teenagers' email accounts. Although monitoring children is needed to ensure safety, mothers have been charged with child abuse and endangerment by leaving their children in the car while they are out shopping, leaving their children in the park alone while they do other things, and leaving their young children home alone. The rationale behind this neglect is that they are left with mobile devices or surveillance cameras to monitor safety. Furthermore, as monitoring often continues to their teenage years, parents have been held responsible for their children's illegal activity online or sexting behaviors resulting in legal obligations from failing to supervise online activity. Children may also be privacy threats to their parents due to their better understanding of technology. Children are usually the savviest technology consumers within their own families and according to the article they act as "sysadmins" within them as well. They may accidentally or intentionally gain access to detailed information of their parents for personal gain, often financial gain. Moreover, elderly parents who are under supervision by their adult children are often ruled out of their own privacy rights. This is due to "granny cams" which are video monitoring equipment to keep tabs on the safety and well-being of elderly relatives. Physical and cognitive impairments make elderly parents or nursing home residents unable to give their consent to being monitored by a relative. Moreover, privacy threats can also arise within friendships. Friends often share intimate details of their lives as the willingness to reveal private information to one another can be misunderstood as closeness in the relationship. By knowing this information, one can easily hack into a friend's account by simply knowing their security questions needed for authentication. Once friendships end each party's personal information are more subject to be compromised.

The article states that there are 4 common features of intimate attacks: emotional ties, copresence of device and account access, dynamic power differentials, and utilizing significant knowledge resources to exploit vulnerabilities. Firstly, intimate attacks are often motivated to seek knowledge of and control over another's behavior. Motivation is also tied with emotions

like jealousy and fear. Emotion plays a strong role in using monitoring tools to exploit vulnerabilities. According to Goffman's use of the term "copresence" it is used to describe situations in which two actors share physical space facilitating 'rich information flow' between them such that people 'are close enough to be perceived in whatever they are doing' (Levy & Schneier, 2020). Shared physical spaces and closeness between threat, victim, and devices create numerous vulnerabilities than the threats reliant of remote access. Copresence allows attackers to access a device physically through shoulder surfing. Attackers can physically watch their victims enter their passwords and use that to their advantage when it comes to installing spyware on their mobile devices. Other information may be shared jointly as a family could only have one computer system in their home or use one common back up system for all their household computers. Copresence is more likely to beat biometric authentication as the article shares that in one published incident a woman unlocked her husband's smartphone by simply placing his hand on the fingerprint reader while he was sleeping. In most cultural norms around the world, men have authority over women or restricted ability. Intimate threats are likely experienced by women and children. In many cases of an intimate threat, the attacker has a more authoritative decision. For example. The person who pays for a phone plan may have the capability of accessing all data for the users within that plan. Furthermore, decisions about installation of smart home monitoring devices are up to the individual who has more control over the household. Geeng and Roesner from the article found that these decision makers often do not consult with other members of the household over these decisions simply because the household is not under their name, or they do not consider them equal in terms of income. Attackers may use intimate knowledge of the victim to gain access to accounts. Information is more likely to be shared during a relationship and may be shared without consent if the relationship ends. Intimate social knowledge denies the existence of certain forms of authentication, which usually rely on personal history. Therefore, attackers may have an ease of access to personal accounts by knowing their security questions needed for authentication.

Ultimately, within the world of cybersecurity and privacy, intimate threats are a significant yet overlooked vulnerability. Due to the intimate nature of the relationships involved in the dynamics of human relationships attackers leverage emotional connections, personal history, and copresence to exploit vulnerabilities. This paper demonstrates the importance of examining these threats from a technological and sociological viewpoint. The studies uncover

the influence of power, behavioral patterns, and technological developments merge to create privacy threats within intimate relationships, families, and caregiving relationships. The proper procedures and implications of these vulnerabilities can ensure protection for the most vulnerable members of society. Recognizing these threats calls for a holistic approach that address security, ethical complications, and societal perspectives in intimate relationships.

WORKS CITED

Levy, K., & Schneier, B. (2020). Privacy threats in intimate relationships. *Journal of Cybersecurity*, *6*(1). https://doi.org/10.1093/cybsec/tyaa006