Volume: 13 Issue: 04 Pages: 5089-5094(2022) ISSN: 0975-0290

Evaluation on Threats to Privacy In Personal Relationships

Dr. Vijay Arputharaj
HOD - Computer Science, School of Science & Information Technology,
Skyline University Nigeria, Nigeria,
Email: phdvij@gmail.com
Mr. Mahmud El Yakub
Department of Computer Science, School of Science & Information Technology,
Skyline University Nigeria, Nigeria,
Email: mahmudelyakub@gmail.com
Mr. Saheed Tunde
Faculty of Computer Science, School of Science & Information Technology,
Skyline University Nigeria, Nigeria,
Email: saheedtzubair@gmail.com
Mr.M.Ponsuresh
Asst. Prof, Department of CSE, Kalasalingam Academy of Research and Education, India.
Email: ponsuresh.techie@gmail.com

ABSTRACT

This commentary paper gives a summary of threats in intimate relationships, which are a type of privacy threats which can result inside families, romantic relationships, friendships, and other close relationships. A lot of popular assumptions about privacy are dispatched in these types of relationships. In fact, plenty of other effective measures tend to fail when applied to these intimate threats. We look into a wide range of intimate relationships and define common features. Therefore, based on these features, we then expand on the ramifications for technical privacy design and policy. Then finally suggest a design recommendation. There are two main security issues in intimate relationships, privacy & authentication related issues. Such privacy issues have been noticed in online learning training in post covid era. A great amount of users in intimate relationships are encountering problems in usability. Most of the issues are due to authentication procedures, sharing passwords, etc.

Keywords – **cyber-security, privacy, relationships, security, threats**

Date of Submission: Dec 05, 2021 Date of Acceptance: Feb 22, 2022

I. INTRODUCTION

The information security society have a tendency to focus on already authorized groups of attackers i.e. companies that track online activities, criminals with the intention of stealing personal data, governmental agencies spying so as to compile information, and hackers who do it for the fun of it. But there are other threats coming from people with much less technically understanding and power but wield intimate knowledge about their intended victims. These sorts of attacks are called intimate threats and they are carried out by one the victim has an intimate relationship with such as a parent, spouse, or friend, etc. There has been little attention granted to these types of attacks from security professionals, but this paper argues that they be treated as a real and primary concern.

These types of threats actually form a large number of the experiences people go through in everyday security and privacy issues. They are so common that they are seen as routine and can often be overlooked even though they can impact the victim's life to a much greater degree than other types of attacks. They also disproportionately target the most vulnerable groups in society such as women, the impaired, children, etc. in a recent survey, about 31% of participants in the survey confessed to perusing through the phones of other people without their permission in just the past year which points out the scale of these type of threats[1]. Another survey discovered that a large majority of parents check their children's internet history and social media [2] [3].

These types of threats also serve as precursors to more well-known types of threats. Some dangers of intimate threats are the loss of personal and or valuable information and can eventually lead to financial fraud, sexual abuse and even a slippery slope of what can be considered acceptable in a relationship [2].

It is important to look deeply into these intimate threats as doing so will benefit the security field. This is difficult due to the technical challenges they hold and the intricate social relationships in which they are borne from.

The goal of this article is twofold: the first of which is to classify and group these types of threats with common features and characteristics as a better understanding of what makes these threats dangerous is imperative to solving them and/or being protected from them. The second is to list out possible ways of nullifying these threats. This doesn't necessarily translate into an actual list of solutions but a conceptual guide to recognizing and nullifying these threats.

Volume: 13 Issue: 04 Pages: 5089-5094(2022) ISSN: 0975-0290

II. INTIMATE RELATIONSHIPS AND MONITORING

Monitoring is a common feature across multiple types of relationships such as in parent-child relationships or in romantic partners, etc. it is common to know the whereabouts of close friends or family members. To know whom they spend time with. Long-term romantic partners even share bank accounts. Those who share housing routinely share phones, computers, and other such devices. It is normal to know each other's passwords.

There are social, cultural, and economic reasons for people to share such intimate details such as it being a cost-effective method to using resources, or it being considered a normal way of showing trust or intimacy to a loved one. And this works vice versa – some partners even like to be monitored as it can be convenient.

It should be pointed out that much of this monitoring is not necessarily ill-intentioned or unwelcomed. It can simply be a reflection of how those in intimate relationships choose to relate among themselves and also the role technology plays within this.

Nonetheless, this raises serious ethical questions. In most situations, there is little doubt as to the illegality of unauthorized access. But this is not the case in intimate relationships - there can be a moral and legal responsibility to look into the safety and security of close ones. This should not blind us to how these types of threats happen and when they are intrusive - it is a very thin line.

Along with the advancement of technology comes the ability to misuse these advancements for ill-intentioned acts. Attackers adopt and repurpose these technologies to serve their nefarious means. Attackers can easily turn to spyware to monitor and stalk their victim's online presence. These spywares have the capability to carry out a wide array of tasks such as recording phone calls, browser history, social media activity, text messages, tracking using GPS, assessing the phone's camera and microphone, among other things. These places a lot of power in the hand of the prospective attacker[4]. These powerful spyware are now routinely called 'stalker-ware' and are freely and openly marketed to the public which facilitates the monitoring of intimate partners, employees, children, and parents, among others. Not too long ago, a Spanish-based company invented a mattress with the capability of notifying a person if their spouse is having an affair by monitoring any suspicious movements on the mattress. The worried party is then notified by text about their spouse's infidelity. This highlights the invasive capability of technology in today's world [5].

With the rise of digital smart home technology, these monitoring and stalking can even give rise to 'gas-lighting'– the act of making one think they are going insane by subjecting them to situations that have no rational meaning. Women have reported the air conditioner turning on and off by itself, the password to their digital lock at their front door changing by itself every day, or the doorbell ringing when there is no one outside. It goes so far as to drive some victims to stay at psychiatric facilities so as to have their mental wellbeing evaluated.

Figure-1: the interconnectivity of today's world.

While there are laws protecting victims of harassment and unsolicited attention from their attackers such as no-contact laws, in today's world, it is very common for friends and families to carry on a conversion over multiple platforms such as Facebook, twitter, discord, WhatsApp etc. all at a time. This only makes the act of monitoring and stalking all the easier for a prospective perpetrator. As all these methods of online communication increase, the law has struggled to come up with a definition as to what constitutes contact. Though law makers and advocates are starting to notify and educate victims that when getting restraining orders against their attacker, they should ask the judge to add smart home devices. Nonetheless, it is difficult to define what constitutes breaking a restraining order when it comes to technology.
Victims of these types of threats cannot turn to the legal system as there is a general lack of will to intervene in the family space. Though there are a few laws protecting victims of non-consensual pornography and spousal violence, there is still a long way to go in protecting other victims.

The word intimate threat is defined broadly in this article going so far as to label what may be described as normal interactions between people as part of these intimate threats. But this is done only to clearly differentiate those who are doing the attacking and those who are defending themselves. A large section of these threats can be described as casual – the attacker may not necessarily be acting with bad intent.

Volume: 13 Issue: 04 Pages: 5089-5094(2022) ISSN: 0975-0290

Figure-2: 3/4 of monitoring and stalking victims are stalked by someone they know

III. DIFFERENT TYPES OF ATTACKERS AND VICTIMS

Intimate relationships are all different by nature. This extends to privacy practices. Here, we list out intimate relationships that are most likely to result in privacy threats.

Intimate partners: It is pretty common and standard for couples to share intimate and private information among themselves – in the modern world, this extends to passwords and online profiles. People routinely have access to their partner's e-mail, social media accounts, etc. it is considered a sign of trust. But what this does is make the task of monitoring and stalking all the easier for a prospective attacker. Partners go so far as to share and sync their data and information across multiple devices that they share. To highlight how wrong this can go, Robert Bentley, the former governor of Alabama was caught being unfaithful as his messages to his mistress were synced onto his wife's iPad.
Intimate threats are commonly found in romantic relationships and can range from casual all the way to abusive over the term of the relationship. Attackers have at their disposal a wide array of tools to use to spy on and control their partners and victims. These tools usually require very little intricate knowledge. They are also joint place. These attackers already have access to their companions' passwords and other secrets, and they rely on this to carry out their nefarious intent. They can also be ingenious, using innocent methods such as child-tracking apps to track their partners. Another method involves using social media to track. Even browser history is another method they can use to infringe on their partner's privacy. In fact, the perpetrator might be a disgruntled ex who stalks his victim with malicious intent. Research has shown that stalkers are share an intimate relationship with their victim turn to much more dangerous methods to achieve their goals than stalkers who don't have an intimate relationship with their victim [5]

It has been noted by over a third of abuse survivors that spyware and GPS locators were a common tool used by their ex-partners to track, stalk, and abuse them. Relationships that take a dark turn to physical and mental abuse usually start by the partner spying on their better half's online presence such as emails, texts, and social media.

It is common is some parts of the world for the surveillance of partners (female mostly) to be even government sponsored. For example, in Saudi Arabia, men have access to a government website which allows them to keep tabs on the females under their guardianship. They can even receive text notifications if any of their female wards were to board a plane [6] [7].

Parents and their children

In today's highly digitized world, parenting faces a challenge as to how to best respond to technological use by teenagers and other children. Finding the balance between independence and parental oversight is becoming more and more difficult. Technology is so ever-present and meshed with the everyday life of children that parents even punish their children by digitally grounding them that is they take away their access to devices and the internet. While technology and the internet offer a wide variety of advantages and benefits, parents are rightfully concerned as to their children's online activity – including whom they interact with, what personal information of theirs is available for the world to see and the more pressing issue of cyber bullying and online safety. In fact, these concerns extend to lawmakers and advocates.

It is normal and even legally required for parents to monitor their children from infancy all the way through adolescence. In fact, it is quite common for parents to be lambasted as being neglectful for allowing their children a certain amount of autonomy due to the busy nature of their lives. To forestall still, parents are forced to digitally track their child's whereabouts and activities. The fear mongering it today's society only exacerbates this. It is quite common for parents to know their child's passwords and online activities. Parents are even legally held responsible for their child's illegally downloading files, creating even more incentive for parents to track their child's activities [8].

The line between parental caretaking and privacy intrusion can be very blurry. Parents do have a duty to supervise their child's activities but there is a limit. Overdoing it can seriously hamper the child's ability to develop a trustful and open relationship with their parents.

There are also less legal and unrelated to parenting reasons for parents monitoring their child such as opening new bank accounts in their name. In fact, research shows that in a majority of cases where a child's identity is misappropriated, it is done by a parent.

Nevertheless, this can also work the other way round with the child being the perpetrator – children tend to be the most technologically proficient in their family and therefore can be trusted by their parents to help with these sort of things such as helping setting up a new device like

Volume: 13 Issue: 04 Pages: 5089-5094(2022) ISSN: 0975-0290

a phone or iPad. It is within the realm of possibility for the child to misuse this trust and gain access to sensitive information like their parent bank details.

Children and their older parents
As children become adults, it becomes their responsibility to care for their ageing parents. As these children become busy with work and other responsibilities, they turn to technology to help with caring for their parents. Technology such as "granny cams", which are cameras that are used for home surveillance, are used to monitor the ageing parent.

The gradual reduction of cognitive activity leaves the elderly unable to give their consent to being monitored. This leaves them exposed even in intimate and private moments such as getting dressed, having a shower, etc. while there have been legislature in seven states of the United States of America, this is still not enough as there is still a legal tendency to accept the rulings of the family as an extension of the ageing person in question.

Caregivers and their patients
As mentioned previously, children can turn to caregivers to provide care to their ageing parents and this becomes another source of intimate threats. These caregivers, ironically, may even use the same tools parents use on their children to monitor them. Though these caregivers may also become victims of monitoring by the government or employees to ensure their providing the very best care to their charges and are also not committing crimes like stealing or harassing the elderly. This also usually occurs using these granny cams, in this case now called nanny cams. There are even applications that can analyses the propensity of a caregiver for drug abuse, bullying, and other types of crimes like stealing.

Friends
By definition, it is normal for friends to share private details and secrets with each other. This can act as an indicator of trust with a person. But as with other types of relationships, friends can become controlling, or the friendship may even turn sour and result in vengefulness. The risk of threats arising becomes even more likely as a result of the inexperience and naivete expected in youth.

IV. FEATURES OF PRIVACY AND INTIMATE THREATS

While individual situations will most definitely vary, these four features are listed below will more or less be present in the different relationships listed above.

1. The perpetrators may carry a wide variety of motivations which are often tied to their emotions.
2. It is inevitable to have access to accounts and devices of partners when there is co-presence.
3. There will always be dynamic power play in all intimate relationships.
4. Perpetrators won't hesitate to use their already deep knowledge of their victim to exploit their vulnerability.

V. POLICY AND DESIGN IMPLICATION

While intimate threats may appear technically unsophisticated, there should be no doubt as to the difficulty of solving them. This difficulty may arise partially as a result of the social complexity and challenge of addressing the underlying threats. They also tend to be diffuse and underhand as opposed to high profile crimes which means they will garner much less attention and concern from safety and privacy professionals[9].

It is important for the creation of legislature and policies and can help mitigate these issues. Also, the question must be asked as to what extent professionals should be held morally and/or legally responsible for the misuse of the technologies which they develop. There is also the problem that it is literally impossible for some type of attacks to ever be detected or even traced[10]. Listed below are some design considerations to help safety and privacy professionals prevent these types of threats:

1. Identify a balance of the multiple interests in intimate privacy and threats.
2. Identify the different information sensitivities.
3. List and enumerate which types of data may unknowingly be transmitted in a visual display.
4. Understand the importance of privacy settings.
5. Understand that sharing preferences can be dynamic.
6. Understand and accept that devices may not be personal and the owner of the device may not be its only user.

The figure below shows the relationship between the features of privacy and intimate threats and the policy and design implication. It relates how recognizing these features may result in a more robust and well thought out design [10] [11].

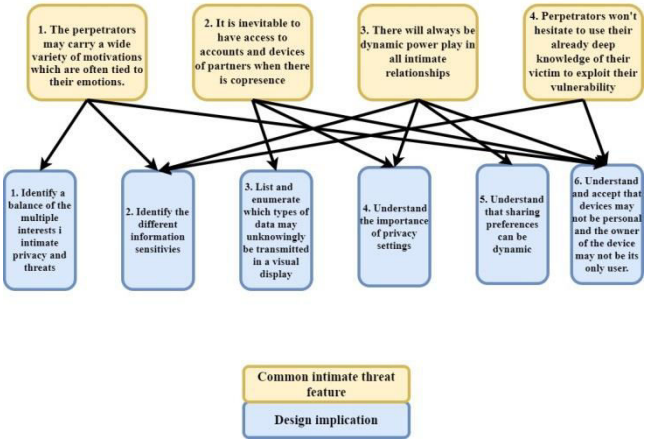

Figure-3: Relationship between the features of privacy and intimate threats

Volume: 13 Issue: 04 Pages: 5089-5094(2022) ISSN: 0975-0290

VI. CONCLUSION

It is most likely that data gathering will increase in the future, most likely as a result of the increase of device sharing in households and increased tracking on social media. The increase of surveillance and tracking devices and applications, and that of the normalization of monitoring in different types of relations makes this a problem to be taken very seriously.

While there has been some heartening attempt in the tech industry to mitigate the prevalence of these applications, it is much more important that these considerations are placed at the system design stage, rather than as a response to attack, after all, prevention is better than cure.

ACKNOWLEDGEMENTS

I would like to thank Dr.Manicka Chezian and Dr. S.SHEEJA for their expert supervision. Both of their wise academic advice and ideas have played an extremely important role in the work presented here and all of my research works. Without their support, this work would not have been possible.

REFERENCES

[1] Levy, K. and Schneier, B. (2020) "Privacy threats in intimate relationships", Journal of Cybersecurity, 6(1). doi: 10.1093/cybsec/tyaa006.

[2] Palarea, R. et al. (1999) "The dangerous nature of intimate relationship stalking: threats, violence, and associated risk factors", Behavioral Sciences & the Law, 17(3), pp. 269-283. doi: 10.1002/(sici)1099-0798(199907/09)17:3<269::aid-bsl346>3.0.co;2-6.

[3] Parents, Teens and Digital Monitoring (2016). Available at: https://www.pewresearch.org/internet/2016/01/07/parents-teens-and-digital-monitoring/ (Accessed: 6 April 2021).

[4] abuse, I. and abuse?, W. (2021) Online and digital abuse - Womens Aid, Womens Aid. Available at: https://www.womensaid.org.uk/information-support/what-is-domestic-abuse/onlinesafety/

[5] Palarea, Russell & Zona, Michael & Lane, John & Langhinrichsen-Rohling, Jennifer. (1999). The dangerous nature of intimate relationship stalking: Threats, violence, and associated risk factors. Behavioral sciences & the law. Vol 17. 269-83. 10.1002/(SICI)1099-0798(199907/09)17:33.3.CO;2-Y.

[6] Saudi Women, Tired of Restraints, Find Ways to Flee (Published 2019) (2019). Available at: https://www.nytimes.com/2019/01/11/world/middleeast/saudi-arabia-women-flee.html

[7] Fetters, A. (2018) Why It's Hard to Protect Domestic-Violence Survivors Online, The Atlantic. Available at: https://www.theatlantic.com/family/archive/2018/07/restraining-orders-social-media/564614/

[8] Parsons, C. et al. (2019) The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry - The Citizen Lab, The Citizen Lab. Available at: https://citizenlab.ca/2019/06/the-predator-in-your-pocket-a-multidisciplinary-assessment-of-the-stalkerware-application-industry/ (Accessed: 7 April 2021).

[9] Thermostats, Locks and Lights: Digital Tools of Domestic Abuse (Published 2018) (2018). Available at:https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html

[10] James Badcock (2016) Smart mattress lets you know if your partner is cheating, The Telegraph. Available at: https://www.telegraph.co.uk/news/2016/04/15/smart-mattress-lets-you-know-if-your-partner-is-cheating/

[11] Young, in Love and Sharing Everything, Including a Password (Published 2012) (2012). Available at: https://www.nytimes.com/2012/01/18/us/teenagers-sharing-passwords-as-show-of-affection.html

[12] Prince Vivek, Rajeev Ranjan (2019), The Discovery for Privacy & Security in Various Big Data Application: A study, Int. Jnl. of Advanced Networking & Applications (IJANA) Special Issue, Volume 10, Issue 5(March-April 2019), PP 78-82.

[13] Lis, A. (2019). Comparison and analysis of web vulnerability scanners (Bachelor's thesis).

[14] Security Onion. URl: https://securityonion.net/ (last visited on 25/07/2021).

[15] P. Raghu Vamsi, Agrah Jain (2021), Practical Security Testing of Electronic Commerce Web Applications, Int. J. Advanced Networking and Applications Volume: 13 Issue: 01 Pages: 4861-4873(2021) ISSN: 0975-0290

Biographies and Photographs

Dr. Vijay Arputharaj J is a Doctorate in Computer Science and HOD – Computer Science, Skyline University Nigeria; He has also completed an integrated Post Graduate, Masters Degree in Software Systems 2005-2010, Bharathiar University. A professional with more than 11 years of progressive experience in lecturing. He is having working experiences in India, Ethiopia and Nigeria. He has also served as Head of Software Engineering Department, Jijiga University, Ethiopia. He has carried out additional responsibilities as Exam Cell Convener, 2012-2014 at VLB Janakiammal College, India by conducting centralized internal exams. He has also undertaken number of training and development programs such as "Enhancing Teaching Skills" conducted by Wipro. Followed by training on "Academic Performance Indicators" at Bharathiar University, India. He is also a part of Educate Community Programme - CSR Activity carried by Skyline University Nigeria, where number of physically challenged and disabled students were benefitted by training programme.

Mr. Mahmud El Yakub, is currently studying in Skyline University Nigeria. He is a junior level student in Department of Software Engineering. Even though he is a

Volume: 13 Issue: 04 Pages: 5089-5094(2022) ISSN: 0975-0290

bachelor student, he has good background and knowledge in various research topics and review articles. He has completed valuable certifications and attended various webinars, seminars etc. He has also been nominated for IEEE Explore student subscription member by Skyline University Nigeria. He is a very active member in Skyline University Toastmasters club. He is also interested in collaborative research projects. He is actively participating in flipped teaching activities and student research publication works. His contribution towards writing this research paper is appreciative.

Mr. Saheed Tunde, is currently working as a Lecturer in Department of Computer Science, School of Science and Technology, Skyline University Nigeria, Kano, Nigeria. He has completed his post graduate higher studies under Bayero University, Nigeria. He has more than 5 years of experience in teaching field. He has extended his service in collaborative research projects and valuable supervision, guidance in under graduate engineering projects. He has taught different courses such as Operating systems, Computer Organization & Architecture, E-commerce, Data structures etc. He is actively participating in lecturing and research publication works. He is also interested in research areas of big data, machine learning, cyber security etc.

Mr. Ponsuresh Manoharan is currently working as an Asst. Prof, Department of CSE, Kalasalingam Academy of Research and Education, India., Also a former Senior Lecturer of Information Technology, Institute of Technology, Jigjiga University, Ethiopia. Before joining Jigjiga University, he served in PSNA College of Engineering and Technology, India. He has completed his higher studies in Sathyabama University, Chennai. He has more than 13 years of experience and valuable publications in teaching and research field. He has extended his service in collaborative research projects, community services and valuable supervision of undergraduate student projects. He taught different courses like Java programming, Android Programming, Python Programming, Integrative programming to name a few. He is actively participating in lecturing and research publication works. He is also interested in research areas of Big Data, Gene Mining, Gene sequence and data analytics etc.