



Online Shopping & Stalking– opportunity to cyber frauds and related harassments – Shoppers perspective and Legal provisions

Amit A. Naik^{1*} and Mamta B. Goswami²

¹ Department of Management Studies, Somaiya Vidyavihar University, Mumbai, India

² Bhagubai Changu Thakur College of Law, New Panvel, University of Mumbai, India

naik.a@somaiya.edu

goswami8mamta2003@gmail.com

Abstract. New age shopping or online shopping leads to many opportunities to cyber criminals to keep an eye on shoppers, known as Cyber- Stalking, through various tactics to manipulate their victims, such as sending flattering messages or love letters initially, sending unwanted advertisements, calls, pop-ups and later which may escalate to threatening or harassing emails if the victim shows signs of resistance or attempts to disengage. Although both men and women can fall victim to cyberstalking, women are disproportionately targeted due to their relatively smaller presence on the internet, leading male users to compete aggressively for their attention. In some cases, stalkers may resort to sending explicit or indecent material or making obscene phone calls. Despite the severity of the consequences, research on cyberstalking remains scarce, and there is a lack of reliable statistics to gauge its prevalence accurately. While cyberstalking predominantly affects women, there is emerging evidence that men can also be victims. This study aims to analyse the experiences and perceptions of online shoppers through explorative methods and by testing relevant hypotheses through statistical techniques along with exploring existing cyberstalking and cyber harassment laws to identify any gaps through literature reviews and explore reasons behind the rising in the incidences and suggesting measures to curb it to lowest possible levels.

Keywords: Cyberstalking, Online Shopping, Online shoppers' perceptions and practices.

1 Introduction

Technological progress serves as a significant asset to humanity, influencing thought processes, behaviours, and responses across various aspects of life. Nowadays, virtually every activity incorporates an essential technological component. The internet has substantially altered people's lives, enabling global communication through email, rapid sharing of documents, and fostering connections with loved ones through social networking sites. While the internet has revolutionized global communication without

boundaries, it also exposes a darker side, evoking concerns of fear, danger, and misuse. The computer, once a tool of innocence, can now function as both an instrument and an active weapon in the commission of crimes. Beyond aiding traditional offenses such as fraud, gambling, defamation, stalking, harassment, and terrorism, computers can be employed as sophisticated tools for criminal activities.

Moreover, the internet has given rise to new forms of crimes, including cyberstalking, harassment, and online deception. Despite its limitless potential, the internet introduces challenges related to security and ethical concerns. The ease of access and anonymity provided by the digital realm contribute to the emergence of these cybercrimes, necessitating a nuanced approach to address and prevent such offenses.

Predictable patterns emerge from certain life events. The birth of a child prompts purchases of diapers and eventually potty-related items. Logical associations also include gaming console purchases leading to the need for games and accessories or contact lens purchases accompanied by lens-cleaning solutions. While this process may seem stalkerish, marketers emphasize its role in personalizing the online shopping experience based on consumer behaviours. It is a method that, when used responsibly, benefits both advertisers and consumers by offering relevant and tailored content.

This research concentrates on understanding how patterns in shopping and online behaviours attracts new tactics of stalking leading to harassment and frauds and its impact on overall consumers and their future shopping behaviours.

2. Review of Literature

The increasing popularity of e-contact in India is driven by the digital acceptance among the new generation through various advertising and promotional channels. In this fast-paced era, time is a critical factor, and electronic contracts (e-contracts) play a crucial role in facilitating efficient transactions between parties. In her book "Cyber Crimes in India," Dr. Amita Verma aims to comprehensively elucidate every facet of cybercrime. She highlights that information technology serves as a double-edged sword, capable of both constructive and destructive uses. Among the various cybercrimes on the rise, cyberstalking stands out as a particularly concerning issue.

Rattan (2015) emphasized the usefulness of e-contracts in e-applications, telephone sectors, and information technology. Electronic contracts have transformed the lifestyles of people in metropolitan cities like Mumbai, enabling the rapid and widespread exchange of information (Karmakar and Pal, 2013).

Desai (2015) highlighted the swift and smooth receipt of information through electronic commerce, strengthening business organizations in terms of wages, locations, and time. E-commerce involves buying and selling commodities through internet facilities, and as it evolves, electronic contracts experience significant growth (Karnatak, 2014).

Krishnan (n.d.) outlined key aspects of e-contracts, including recognition of offers, liability, damages, acceptance, and considerations. Alexander (2013) emphasized the legal importance of fulfilling rules according to the code of conduct for a contract to be considered valid. Advertisements on various websites may or may not be regarded as offers. Althaus et al. (2012) discussed the concept of offers, especially in the case of unauthorized persons, as a reward or treat. The examination of the supply of conversations between parties determines the legal binding nature of the agreement.

Customers responding through email or online forms may initiate offers, which sellers can accept through confirmation or adherence to government-prescribed codes of conduct. In their book "Cyber Crimes against Women in India," Debarati Halder and K. Jaishankar delve into the experiences of numerous Indian women who have fallen victim to various forms of cybercrimes. Despite constitutional guarantees of gender equality in India, women often find themselves relegated to second-class citizenship within a patriarchal societal framework.

Kobets & Kristina, 2018 expressed Cyberstalking is a criminal offense, and those who engage in it can be held accountable. Like any crime, it comprises two essential elements: *mens rea* (the mental state) and *actus reus* (the physical act). The *mens rea* in cyberstalking involves a deliberate intent to cause emotional distress or fear, effectively making the victim uncomfortable even in their own home or safe spaces. Social media platforms facilitate information sharing among users, but they also expose individuals' personal information, which can contribute to these harmful behaviors.

3. Research Methodology

The global prevalence of cyberstalking and online harassment necessitates urgent attention, extending beyond India. This study aims to categorize the various forms of cyberstalking and the profiles of perpetrators, emphasizing the interconnectedness between this egregious crime and various other criminal activities.

Furthermore, the research seeks to identify the root causes of cyberstalking and proposes viable solutions to counteract this escalating menace.

The study is based on Primary and Secondary sources of data. Under Primary sources, data will be collected by survey techniques after defining research Universe and Samples. Samples will be selected on the basis of convenient and snowball techniques. Given the nature of the research, there is a substantial dependence on internet sources, particularly for information on cyberstalking complaints and recent amendments, as these details are frequently updated and readily accessible on regularly updated websites. Additionally, the study incorporates some self-perceived views to enrich the analysis.

3.1 Objectives

The research purpose is to get the following objectives with the help of Primary and Secondary data.

1. To know the nature of Online Stalking, its purposes and use in business generations.
2. To understand the historical perspective, developments, and international perspectives of Online Stalking.
3. To understand Online shoppers' perspective towards Online stalking and its effects
4. To analyses overall perspectives and challenges to have robust mechanisms to deal with repercussions of Online stalking.

3.2 Hypotheses

Following hypotheses were drafted for the testing purpose based on data collected.

- # H01 – Online stalking does not lead to mental harassment and irritation to the user
- # H11 – Online stalking leads to mental harassment and irritation to the user.
- # H02 – Online stalking does not result into more purchasing and more business
- # H12 – Online stalking results into more purchasing and more business

4. Data Analysis & Interpretations

In the analysis maximum people,45%, have experienced that they have been stalked, 5% were not even aware whether they were been stalked or not, 20% respondents were not stalked at all, whereas 10% were not ready to respond. (refer figure 1)

Table 1: Do u have social media accounts

Row Labels	Do u have social media accounts
Whatsapp	10
Whatsapp;Facebook	10
Whatsapp;Facebook;Instagram	10
Whatsapp;Facebook;Instagram;Telegram	10
Whatsapp;Facebook;Instagram;Twitter (X)	5
Whatsapp;Facebook;Instagram;Twitter(X); You Tube;Telegram	20
Whatsapp;Facebook;Instagram;Twitter (X); You Tube;Telegram;Other	5
Whatsapp;Facebook;Instagram;We Chat;Telegram	5
Whatsapp;Facebook;Instagram;You Tube;Telegram	15
Whatsapp;Facebook;Other	5
Whatsapp;Instagram	5
Whatsapp;You Tube	5
Grand Total	105

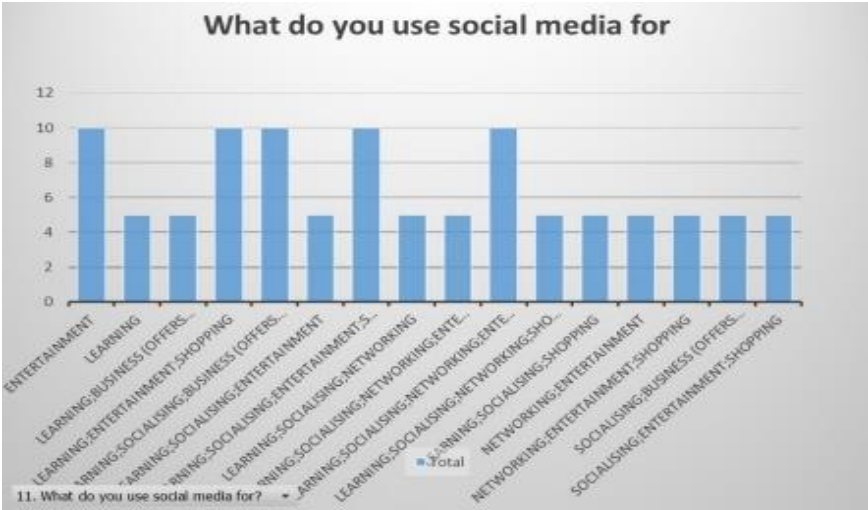


Figure 1: What do you use social media for

There are various purposes for respondents to use social media like entertainment, learning, business, shopping as well as socializing, networking and so on. Maximum people out of respondents have used social media for the learning purpose, second highest is the socializing, next highest is the networking and least is for the entertainment and shopping, very few of them have used social media for the business purposes.

There are various purposes for respondents to use social media like entertainment, learning, business, shopping as well as socializing, networking and so on. Maximum people out of respondents have used social media for the learning purpose, second highest is the socializing, next highest is the networking and least is for the entertainment and shopping, very few of them have used social media for the business purposes.

4.1 Testing of Hypotheses

To test the first hypothesis, Non – parametric test, Chi square is used. As per the calculations Mean value is 2.53 with standard error is 0.11 and Sigma value i.e. standard deviation is 1.22 which signifies the collected data is closely knitted.

Chi square calculated P value is greater than Chi square tabulated value at 95 % level of confidence, so null hypothesis i.e. Online stalking does not lead to mental harassment and irritation to the user is rejected and alternative hypothesis is accepted i.e. Online stalking leads to mental harassment and irritation to the user.

Table 2: Descriptive Statistics

Descriptive Statistics	
Mean	2.538461538
Standard Error	0.119841722

Standard Deviation	1.222150555
Sample Variance	1.493651979
Kurtosis	-0.036340944
Skewness	0.820155043
Confidence Level(95.0%)	0.23767779

In order to signify the results, parametric test – t test also known as Students' t test is also applied. The calculated t stats value is 3.9 which is greater than 2, signifies strong difference between two sample means and discredited null hypothesis, which results into rejection of H01 i.e. Online stalking does not lead to mental harassment and irritation to the user and accepted alternative hypothesis, which is in line with chi square test results.

Table 3: t-Test: Paired Two Sample for Means

Mean	2.523809524	2
Variance	1.501831502	0.480769231
Observations	105	105
Pearson Correlation	0.056579321	
Hypothesized Mean Difference	0	
df	104	
t Stat	3.907920759	
P(T<=t) one-tail	8.2978E-05	
t Critical one-tail	1.659637437	
P(T<=t) two-tail	0.000165956	
t Critical two-tail	1.983037526	

Hypothesis 2

H02 – Online stalking does not result into more purchasing and more business

H12 – Online stalking results into more purchasing and more business

Table 4: Has stalking impacted your choice(s) of selection.

Mean	2.047619048
Standard Error	0.056420959
Standard Deviation	0.578142789
Sample Variance	0.334249084
Kurtosis	0.059099275
Skewness	0.001150204
Confidence Level(95.0%)	0.111884879
Online stalking offers advantage like personalized offers/ advertisements leads to [Influence your purchasing decisions]	

Mean	2.142857
Standard Error	0.114377
Standard Deviation	1.172018
Sample Variance	1.373626
Kurtosis	1.306284
Skewness	0.995296
Confidence Level(95.0%)	0.226814

Online stalking offers advantage like perso0lized offers/ advertisements leads to [Draws your attention and lead to diversion]	
Mean	1.857143
Standard Error	0.075869
Standard Deviation	0.777429
Sample Variance	0.604396
Kurtosis	-0.10158
Skewness	-0.37039
Confidence Level (95.0%)	0.150452

Table 5: t-Test: Paired Two Sample for Means

	<i>Variable 1</i>	<i>Variable 2</i>
Mean	2.047619048	2.476190476
Variance	0.334249084	1.79029304
Observations	105	105
Pearson Correlation	-0.15389466	
Hypothesized Mean Difference	0	
Df	104	
t Stat	-2.8570598	
P(T<=t) one-tail	0.002582372	
t Critical one-tail	1.659637437	
P(T<=t) two-tail	0.005164744	
t Critical two-tail	1.983037526	

For the testing of 2nd hypothesis again same line of tests were used i.e. parametric test. Whereas non-parametric test which based on experimental values is purposely avoided. The t test for two sample means indicates, P value – 2.85 which indicates considerable difference between two sample means and results in to rejection of null hypothesis i.e. Online stalking does not result into more purchasing and more business and accepted alternative hypothesis i.e. Online stalking results into more purchasing and more business

5. Findings:

Comprehensive summary of various aspects of online presence and its impacts from the survey findings covers demographics, behaviours, attitudes, and experiences of respondents regarding online activities, highlighting the complexities and nuances involved in navigating the digital world.

1. A survey targeted 18 to 50-year-olds with online presence, revealing 35% aged 35-45, 36% aged 26-34, 20% aged 46-50, 15% aged 45+, and 5% aged 18-25.
2. Users had varied employment statuses: 45% employed, 35% not employed, and 25% self-employed, with employed individuals showing greater online presence, while students, comprising a significant portion of the not employed group, had the lowest presence.
3. Half of the respondents were married, with 30% being married homemakers, 15% students, and 5% unmarried, indicating a majority being married individuals.
4. Among respondents, 62% were male and 38% female, all maintaining digital presence through various social media accounts, notably WhatsApp being most prevalent for communication across different social strata, highlighting its widespread popularity and utility, while fewer utilized platforms like Telegram and Twitter.
5. Analysis reveals 45% of respondents have experienced being stalked, 20% were not stalked, 5% were unaware of being stalked, and 10% did not respond.
6. Despite the potential for harassment with online presence, 70% of respondents reported no harassment, while 20% confirmed harassment, 10% were unsure, and 5% declined to respond.
7. Despite various impacts of social media influence, 55% of respondents claimed no effect, while 35% acknowledged its impact, with 15% uncertain about its influence on them.
8. Despite the varying extent of social media influence on behaviour, 70% responded that their behaviour is seldom affected, 5% acknowledged regular influence, and 30% claimed no influence at all.
9. The duration of social media presence significantly influences respondents' behaviour, with 35% spending one hour, 50% spending 1-3 hours, 15% spending 3-5 hours, and only 5% spending over 5 hours, suggesting varying levels of impact based on time spent.
10. Respondents utilize social media for diverse purposes including learning, socializing, networking, with learning being the most prevalent, followed by socializing and networking, while entertainment, shopping, and business purposes are less common.
11. Frequency of social media presence correlates with higher risks of harassment and stalking, as 95% of respondents are active on social media daily, while only 5% are rarely present.

12. When queried about the correlation between online presence, stalking, and physical intrusion, 20 respondents agreed, 15 disagreed, 10 strongly agreed, and 60 reported no such experiences among 105 respondents.

6. Suggestions & Recommendations

- A specific and comprehensive legislation targeting cyberstalking is urgently needed. The existing Indian Penal Code of 1860 is outdated and ill-equipped to address the evolving landscape of cybercrime. To effectively combat cybercrimes, including cyberstalking and online harassment, a new approach is essential.
- Requirement of uniform laws: The global nature of cyberstalking necessitates a unified and consistent approach across all nations. It is imperative for countries worldwide to collaborate in tackling this pervasive issue. The pressing need is for international laws that set a universal standard for addressing cyberstalking and online harassment.
- There is a widespread lack of understanding among the public regarding the various forms of cyberstalking and the available solutions to combat it.: Many individuals are unaware of which specific behaviours constitute cyberstalking under existing laws. Simply enacting legislation is not enough; it is crucial for people to recognize and report instances of criminal behaviour.

7. Conclusion

In today's era of information and communication technology, the internet and mobile applications have become pivotal. Virtually everyone experiences both the positive and negative impacts of this digital transformation. Alongside the internet, computers have created a virtual realm where individuals can communicate uniquely. Social networking sites have established virtual communities, which some find more engaging than the physical world. The internet has bridged geographical gaps, enabling global communication. However, with these advantages come drawbacks, including virtual criminal activities. Just as in the real world, the virtual environment hosts both good and bad actors.

While stalking has recently gained legal recognition, its dynamic nature is a product of the twentieth century. Criminal behaviours has proven highly

adaptable to technological advancements, such as credit cards, mobile phones, and computer fraud. Stalking has evolved into cyber stalking, leveraging the internet and electronic media to pursue, harass, or contact individuals in unwanted ways. Although cyber stalking may not involve physical presence, it can in still fear and offers perpetrators various advantages, including easy contact and access to personal information.

Online stalking affects both men and women, with women comprising the majority of victims due to their smaller representation in the online population. Male users often compete vigorously for female attention, employing various tactics to manipulate victims, such as sending letters, compliments, or even threats and indecent messages. The anonymity provided by the internet facilitates such behavior, posing risks of unwelcome scrutiny to online personalities.

References

1. Viswanathan, A. (2015). *Cyber law: Indian and international perspectives on key topics including data security, e-commerce, cloud computing, and cyber crime*. Lexis Nexis Publication.
2. Miftna, A., Conrad, M., & Gipson, M. (2017). The social, legal, and technical perspective of cyber stalking in India. In *Proceedings of the 15th International Conference on e-Society*. International Association for Development of the Information Society. Available at www.ladisportal.org (accessed April 25, 2020).
3. Barkha, & Mohan, U. R. (2010). *Cyber laws and crimes*. Ashia Law House.
4. Dayal, D. P. (2005). *Spam attacks, cyberstalking, and abuse*. Dominant Publishers and Distributors.
5. Goel, H. (2014). *Law and emerging technology (Cyber Law)*. New Era Law Publications.
6. Chatterjee, I. (2018). *Law on information technology*. Central Law Publications.
7. Rattan, J. (2020). *Cyber laws & information technology* (8th ed.). Bharat Law House.
8. Goel, H. (2007). *Cyber crime* (p. 18). Rajat Publication.
9. Goel, H. (2014). *Law and emerging technology (Cyber Law)*. New Era Law Publications.
10. Chatterjee, I. (2018). *Law on information technology*. Central Law Publications.
11. Lloyd, I. J. (2020). *Information technology law* (9th ed.). OUP Oxford.
12. Mishra, J. P. (2014). *An introduction to cyber law*. Central Law Publication.
13. Richards, J. R. (1999). *Transnational criminal organizations, cyber crime and money laundering*. CRC Press.

14. Gaur, K. D. (2016). *Textbook on the Indian Penal Code* (811). Universal Law Publishing.
15. Mani, K. (2019). *Legal framework on cyber crimes*. Kamal Publishers.
16. Seth, K. (2016). *Protection of children on the internet*. Universal Law Publishing – An imprint of Lexis Nexis.
17. Seth, K. (2019). *Computers, internet and new technology laws*. Lexis Nexis Publication.
18. Bora, K., & Borah, U. (2021). *A handbook of cyber law & information technology in India* (p. 102). Notion Press.
19. Kobets, P., & Krasnova, K. (2019). Cyberstalking: A Public Threat, Key Factors, and Prevention Strategies. *Przegląd Wschodnioeuropejski*, 9(2), 43–53. <https://doi.org/10.31648/pw.3001>

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

