

Designing a Privacy-Aware, Secure Peer-to-Peer E-commerce Platform for College Students: An Analysis of Privacy and Security Issues in Existing P2P Platforms and Their Impact on Social Environments

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Ayub Shahab

Spring 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

ADVISORS

S. Travis Elliott, Department of Engineering and Society

Introduction

The sphere of online activity has undergone a drastic surge in recent times, thanks to the ever-expanding digital landscape that allows individuals to participate in a number of online activities. Individuals can practice a wide variety of daily functions such as, but not limited to, e-commerce transactions, media streaming, payment processing, and much more, all from the comfort of their homes. Furthermore, examining the composition of said online participants, it is not exclusively limited to adults that practice sound judgment and cautiousness, but rather youngsters and adolescents are equally, if not more, likely to engage in online activities, which undoubtedly raise a wide variety of concerns. At the forefront of these concerns is the ever-increasing presence of fraudulent activity that individuals now need to navigate when participating online. College-age young individuals are especially susceptible to falling prey to fraudulent activity as they lack the experience and wisdom of their older counterparts. Therefore, as a response to the growing digital trend and the greater number of individuals that choose to opt online, it has become a critical imperative to emplace a more rigid and secure digital infrastructure that can effectively shield and safeguard individuals participating in the online social norm. The purpose of this paper is to explore this phenomenon of online scamming of youngsters in the context of the rapidly growing e-commerce phenomenon. Specifically, this paper will analyze the privacy and security issues in existing P2P (peer-to-peer) e-commerce platforms and their adverse effects on the respective, predominantly young-adult user base. Addressing these issues, this research aims to develop a blueprint for a more privacy-focused, secure peer-to-peer platform that harbors a safe online environment, one that is specifically for college students.

The Rise of Online Scams

As introduced above, the rise of digital technology has heightened the exposure of individuals to fraudulent activity when surfing online, particularly on P2P e-commerce platforms, which already demand particular and careful attention when navigating. The stakeholders of these platforms, which primarily encompass youngsters, adolescents, and young adults, such as college students, are at a heightened risk of falling prey to fraudulent schemes compared to their older and much more shrewd counterparts. Young adults, specifically college students, serve as an ideal stakeholder when discussing the issue of falling prey to fraudulent activities, as their sheer number and desire to purchase goods with limited funds result in them navigating existing P2P platforms. According to the National Center for Education Statistics (2017), roughly 19.4 million students are currently enrolled in colleges and universities, and this number is only expected to grow in the future. One thing that all students pursuing postsecondary education have in common is their need to interact in an e-commerce marketplace to obtain items they desire. Since college students have limited financial access, the most popular places for them to browse are existing P2P platforms like Facebook Marketplace and OfferUp®. However, that is where some of the issues with such wide-access marketplaces become prevalent. Issues such as a lack of security and privacy are breeding grounds for scams.

College students are especially likely to fall prey to these scams, as their limited financial access, compounded with their lack of experience in making financial decisions, results in them making choices that prove to be harmful to themselves. To further understand how exactly online activity promotes fraudulent activity, technological determinism can be leveraged. Although this complex dynamic is explained in detail below, in short, the very nature of online activity invites fraudulent activity. As more and more businesses and individuals choose to opt online because it

is faster, more convenient, anonymous, and has a wider outreach, swindlers routinely target online platforms as it is easy to gain trust and affect a mass audience. Furthermore, the newer generation, specifically college-age young adults, have grown up in the digital age and are more easily misled by the dishonest antics of scammers. In an article published by ProPublica discussing the growing rate of scams on Facebook Marketplace, the non-profit news giant quotes a statistic from the bureau's Internet Crime Complaint Center (IC3) stating that in just 2020 alone, there have been a total of "792,000 total incidents [regarding online fraud], which is an increase of 70% from the previous year" (Silverman et al., 2021). This alarming increase in fraud cases on a monumental platform like Facebook highlights the compromised security of these platforms and how users consistently fail to recognize different scams. It becomes evident that existing P2P e-commerce platforms do not provide a safe environment for users to engage in e-commerce activity. This can be due to a variety of reasons, but the primary culprit is individuals, especially college students, not having the experience or being perceptive enough to see through scams.

College students that choose to acquire goods and services from these online e-commerce platforms frequently find themselves navigating in an adverse environment where, at any moment, they could fall victims to scams. The growing trend of consumers choosing to shop online also does not pair well with the issues of privacy and security that persist on these existing peer-to-peer e-commerce platforms. According to the United Nations Conference on Trade and Development (2021), all digital retail platforms have experienced a surge in e-commerce activity where consumers are choosing to go "digital." The UNCTAD emphasizes that, following the events of COVID-19, the influx of digital shopping led to an increase in "ecommerce's share of global retail trade from 14% in 2019 to about 17% in 2020." The failure of existing peer-to-peer

e-commerce platforms to adequately protect and safeguard their users has created a grave danger for current users, especially in light of the recent influx of online shopping. It is imperative that these platforms either be revamped to prioritize security and privacy at their core or that a new platform be designed specifically for students that addresses these concerns head-on. This study aims to examine the privacy and security concerns that exist on P2P platforms today and how they affect social settings, while also outlining a proposed solution that takes these concerns into account and addresses them. This research will achieve this through the aid of two socio-technical frameworks: technological determinism and techno-social.

Framework: Technological Determinism

The growing number of consumers choosing to shop online highlights the technological determinism at play where consumers will engage in e-commerce activity online as opposed to in person for the sake of efficiency and convenience. Technological determinism is the idea that society and technology have a causative relationship where "technology is a driving force of culture in a society and it [influences] its course of history" (Communication Theory, 2018). Through this lens, the rationale for the growing digital trend, particularly in online marketplaces, becomes clear, as traditional brick-and-mortar stores have become less efficient in comparison. The inherent attributes of online marketplaces and digital transactions, such as affordability, accessibility, and wide outreach, propel their continued growth and evolution. Technological determinism emphasizes that technology has the ability to shape society in predictable and deterministic ways and, in contrast with the socio-technical framework, works independently of social and cultural variables. However, by extension of this very definition, it is reasonable to believe that, in some cases, this causative relationship will be beneficial and adverse in other instances. For example, a beneficial societal outcome of technology is advances in medicine that

have led to the development of life saving treatments. Adversarial societal outcomes would include increased cyberattacks due to the ever-increasing online presence. In the case of online e-commerce, the cause-and-effect relationship cannot be labeled at either extreme of the spectrum, as the effects of going digital ultimately depend on the checks that are in place to protect the users, as well as the technology itself, from the implications of failing to protect its users.

If a technology is evolving in a way that is increasingly disregarding the safety and security of its users, then it needs to be amended. On the other hand, if a technology brings relief and efficiency to the daily lives of individuals, then it is further improved and expedited to further promote the good of stakeholders. Such aspects in regards to P2P platforms will be discussed in detail shortly; however, there is one detail that needs to be discussed when analyzing this scenario through the lens of technological determinism. Technological determinism often oversimplifies the complex relationship between technology and society by placing an emphasis on technology first, whereas in reality, social and cultural factors can also shape and impact the development and use of technology. However, it is important to note that both frameworks, technological determinism and techno-social, play a critical role in understanding online e-commerce platforms and technology in general, as one explains its development while the other examines its impact on society through a cause-and-effect relationship. Understanding the complex relationship between technology and society helps us understand the larger implications of P2P platforms if a technology fails to uphold its social responsibility of protecting its users.

Framework: Socio-technical

Discussing P2P platforms strictly through technological determinism results in a limited analysis as it fails to understand the duality of the causal effect relationship between e-commerce

platforms and the stakeholders that partake in them. Both the stakeholders—the users navigating the platform—as well as the platform itself can serve as cause and effect. To analyze this complex relationship, the socio-technical framework can be deployed to determine the extent of each participating force's influence on the other when categorized as the catalyst. "Human experience, [which can serve as either the cause or the effect], is at the same time technologically infused and highly social. Life is therefore techno-social in the fullest sense of the word. [The hyphenation of this word calls] for equal attention to both the technological and the social and to their equivalent importance in the examination and understanding of modern life. The technological and the social are in such intimate interaction, constantly influencing one another, [that either subject cannot be discussed without demanding attention to the other]" (Chayko, 2021). Clarified, the techno-social paradigm sees technology and society as co-constitutive and mutually forming. Technology and society are intertwined and mutually influence each other rather than being separate entities. According to this perspective, social factors like culture, politics, and economics shape and influence technology rather than the other way around, which then influences and molds social practices, relationships, and institutions.

The techno-social framework acknowledges that technology is not a neutral instrument but is instead infused with social norms and values and can be used in ways that both replicate and challenge preexisting social structures. This view is contrasted with technological determinism, which prioritizes technology as the primary force of influence. This framework emphasizes the requirement for a more thorough comprehension of the intricate and dynamic connection between technology and society, as well as the importance of considering the social implications of technological developments. As mentioned earlier, technological determinism and the techno-social framework are not competing forces but rather work collectively to

carefully analyze a given technology; specifically, an analysis of online e-commerce marketplaces with one framework without the other would be incomplete.

Impact of Online Scams on Different Social Groups

In an article published by The New York Times on the likelihood of the young falling for scams, cowriter Ron Lieber provides a statistic from the Federal Trade Commission that highlights that 44% of people ages 20 to 29 lose money to fraud, which is more than double the 20% of people ages 70 to 79 (Lieber, 21). Although the age gap between the participants in the study is quite substantial, there is a clear distinction: the young simply do not practice the same sound judgment that their older counterparts do. Given the statistics provided by the New York Times, an argument can be made that the overall number of elderly individuals accessing online marketplaces is considerably lower than that of the younger, tech-savvy generation. Although this may be true, the ratio of young adults falling prey to online fraud is still considerably higher. This phenomenon can be explained by the trust vs. mistrust factor, which is discussed in depth below and analyzed through the lens of the techno-social framework. In short, older individuals grew up with brick-and-mortar stores and simply did not trust online transactions. On the other hand, the younger generation has been brought up in the digital age and is not preceptive enough to see through well-thought-out scams.

Further adding to the problem is the failure of existing peer-to-peer (P2P) e-commerce platforms to provide the expected level of privacy and security, thereby fostering a false sense of trust that ultimately allows college students and their peers to fall vulnerable to fraudulent schemes. The advancement in online capabilities and the consequent growth in the number of individuals participating in peer-to-peer e-commerce platforms have revealed many concerns about the privacy and security of these platforms, specifically among college students and other

young adults who may be more susceptible to fraud. Current P2P platforms that lack a robust and secure digital infrastructure foster a false sense of confidence in users, making them more susceptible to scams.

In-Person to Online Transition: Causes & Consequences

The gradual use and ultimate reliance of individuals on online peer-to-peer e-commerce platforms is largely driven by the concept of technological determinism. Technology has facilitated a paradigm shift away from conventional brick-and-mortar stores towards an online emphasis as factors, such as monumental expenses linked to physical storefronts, as compared to minimal expenditures on running online servers, as well as a substantial worldwide outreach without regard to the store's physical location, have rendered it completely infeasible to continue to conduct business without a digital presence. Conversely, online peer-to-peer e-commerce platforms, such as the ones discussed, Facebook Marketplace, OfferUp, and many more, are considerably less taxing on stakeholders' pockets and therefore easier to establish and facilitate. Furthermore, it can be argued that by serving as a middleman between producers and consumers, or, in the case of P2P e-commerce platforms, buyers and sellers, there is no cost associated with vendors or users listing merchandise. Presumably, serving as a middleman is of greater interest to a business as the platform can retain a modest percentage of transactions and generate other forms of revenue.

Focusing on the users as stakeholders, the consequences of technological determinism in light of P2P e-commerce platforms are not downright optimistic. As discussed previously, the effects simply depend on the effort of the online platform to maintain its reputation by safeguarding its users against potentially fraudulent activity. Discussing existing peer-to-peer platforms further, the ProPublica news-media outlet highlights that "the company's confidence

about the safety of its platform is misguided," as the company's primary line of defense is automated software that "frequently fails to ban obvious scams" (Silverman et al., 2021). A fundamental determinant that governs the prosperity or failure of an online e-commerce platform is linked to the level of confidence and trust of the respective user base. These elements play a pivotal role in fostering an atmosphere of reliability and dependability, which are indispensable to the attainment of long-term viability and success in the digital marketplace. Abiding by technological determinism, the platform's failure to protect its members against scams will falter consumers' confidence in trusting online e-commerce platforms. As we have discussed previously, this shift from in-person commerce activity to online commerce has large implications, whether beneficial or adversarial, depend on the actions that the platform adopts in terms of policies to safeguard its respective users. However, the adverse effects require greater consideration and can't be overlooked due to their detrimental effects on society as a whole.

Discussing the quote from ProPublica, this lack of confidence of users in cybershopping will persist from platform to platform and will have a detrimental effect where consumers are more cautious than ever and may not take advantage of certain scenarios as they have been scarred from previous experiences. Overall, the proliferation of online peer-to-peer e-commerce platforms is a testament to the dynamic interplay between technology and societal and economic structures; however, strictly analyzing this relationship through the lens of technological determinism will undermine the societal influence at play. Therefore, to fully discuss the implications of P2P platforms and their failure to uphold societal norms and safeguard the privacy of their users, it is critical to analyze the given scenario through the lens of the socio-technical framework.

Trust vs Mistrust

The techno-social framework focuses on the relationship between technology and society and how the two influence and are influenced by each other. On the one hand, technological determinism highlights the growing trend of consumers going digital as they choose to shop online for the sake of efficiency and convenience. On the other hand, the techno-social framework helps us understand how technology impacts our social lives, and vice versa, and how online shopping scams ultimately have a detrimental effect on the larger society as social interactions occur in a heightened state where an online platform's consistent failure to protect its users breeds fear and uncertainty in individuals. Discussing the topic of trust, the trust-vs.-mistrust factor can be a significant difference in how younger and older generations perceive and use online e-commerce platforms. This factor is also attributed to the fact that a greater percentage of college-age young adults fall victim to scams as compared to their older counterparts. The older generation, which has grown up with brick-and-mortar stores and other traditional forms of commerce, may be more trusting of established brands and may view online transactions with more skepticism. In sharp contrast, college-age young adults tend to exhibit behaviors and personalities that include a higher degree of familiarity with online transactions and a greater inclination to trust online platforms. Oftentimes, this inclination undermines their cautiousness and renders them unable to identify illicit activity.

Security and privacy are two closely related aspects of online peer-to-peer e-commerce platforms, where security encompasses the measures taken to protect a respective platform from unauthorized access, data hacks, and fraudulent activity, while privacy refers to the protection of user data. Security and privacy are two sides of the same coin, and failing to address one has detrimental effects on the other. Failure to address either one results in a lack of user trust. To

further emphasize the gravity of this matter, ProPublica also highlights that the 400 low-paid contractors deployed to resolve matters regarding scams sometimes engage in unsolicited activity themselves, where workers often "spy on romantic partners and commit other privacy violations" (Silverman et al., 2021). Continuing the argument of user confidence, the framework of techno-social life can be utilized in conjunction to emphasize that social interactions within a community will also be adversely affected as individuals feel they are constantly being monitored.

The adverse implications of failing to establish a secure platform discussed so far have been mild, but Silverman from ProPublica also highlights that in terms of illegal and criminal activity, scams are only the beginning; more significant crimes can also take place on these unmonitored, less secure platforms. The author states that "since the start of the pandemic, criminals across America have exploited the marketplace to commit armed robberies and, in 13 instances identified by ProPublica, homicide" (Silverman et al., 2021). The evidence provided serves to highlight the drawbacks of using existing e-commerce platforms and emphasizes that although technological determinism advocates for online e-commerce activity, the failure of platforms to uphold social responsibility to protect their users ultimately has a detrimental impact on the techno-social relationship. No proprietary technology can serve as a complete beneficiary to the stakeholder collective, regardless of whether that stakeholder is a participant in the technology or one that produces it; each stakeholder can serve as a causality at either extreme on a causal-effect map, where failure to address the needs of the other can determine the eventual deposition of proposed and previously adopted technologies. In light of the aforementioned evidence, it is apparent that the complex relationship between P2P platforms and the participants that partake necessitates an analytical approach that considers both technological determinism

and socio-technical theory, where failure to account for the requirements of either theoretical perspective results in a constrained analysis.

Conclusion

The recent growth of online platforms to provide goods and services pertaining to all aspects of social life has caused a shift in human shopping patterns where, more than ever before, individuals are choosing to engage in online platforms to address their needs. However, this proliferation of online peer-to-peer platforms has brought about a multitude of security and privacy concerns, which in turn pose significant risks that individuals must navigate. The rampant incidents of fraudulent activity have fueled a loss of trust in individuals in regards to P2P platforms, leading to a broader disillusionment with society and a lack of trust in others as a whole. Although arguably there are benefits to engaging in a peer-to-peer e-commerce platform, namely diversification, ease-of-use, and variety, the existing platforms are not ideal as they fall short in protecting their members against malicious actors, ultimately undermining the very confidence these platforms require as a foundation for success. This research paper has critically examined existing solutions through the prism of technological determinism and socio-technical theory, delving into a variety of reasons behind current platforms' inability to foster a safe environment and the social consequences that result in not doing so. The privacy and security concerns of the users should be central to all P2P platforms, and existing as well as future platforms should abide by this convention in an effort to establish a climate of trust and confidence, which is paramount for ensuring the success of any peer-to-peer e-commerce platform.

References

- Chayko, M. (2021). *Superconnected: the internet, digital media, and techno-social life* / Mary Chayko (Third Edition, p9). Sage Publications Ltd.
- Communication Theory. (2018, April 23). *Technological Determinism*. Retrieved March 16, 2023, from <https://www.communicationtheory.org/technological-determinism/>
- Lieber, R. (2021, June 25). *The young fall for scams more than seniors do. Time for a warning*. Retrieved March 16, 2023, from <https://www.nytimes.com/2021/06/25/your-money/young-seniors-scams-warning.html>
- National Center for Education Statistics. (2017, December 31). *Fast Facts*. Retrieved March 16, 2023, from <https://nces.ed.gov/fastfacts/display.asp?id=372>
- Silverman, C., Thompson, A. C., & Elkind, P. (2021, September 22). *Facebook Grew Marketplace to 1 Billion Users. Now Scammers Are Using It to Target People Around the World*. Retrieved March 16, 2023, from <https://www.propublica.org/article/facebook-grew-marketplace-to-1-billion-users-now-scammers-are-using-it-to-target-people-around-the-world>
- UNCTAD. (2021, March 15). *How COVID-19 triggered the digital and e-commerce turning point* / UNCTAD. Retrieved March 16, 2023, from <https://unctad.org/news/how-covid-19-triggered-digital-and-e-commerce-turning-point>