DATA PHISHING OF CONSUMERS: A CHALLENGE WITH THE ADVANCEMENT OF AI WITH REFERENCE TO THE INFORMATION TECHNOLOGY ACT, 2000

Naomi Madhukesh, Christ (deemed to be University)

ABSTRACT:

We will only experience great inconvenience if we decide to quit using the internet completely after learning about all of these cybercrimes. Consumer data phishing is a serious issue that has emerged as a result of the big data explosion and the quick development of artificial intelligence (AI). This problem creates serious legal ramifications in addition to worries about data insecurity, especially in light of the Information Technology Act of 2000. In light of the rise of artificial intelligence and big data, this paper explores the intricate issues surrounding data security and privacy, drawing parallels with George Orwell's dystopian classic "1984." The study aims to examine the techniques employed by cybercriminals, evaluate the effectiveness of the Information Technology Act of 2000, and conduct a comprehensive analysis of the current state of data phishing. The report also looks at how AI might both exacerbate and lessen data phishing situations. It also examines legal and regulatory frameworks and identifies issues that law enforcement agencies must deal with. In addition, the study looks at consumer awareness and education initiatives, explores best practices from other areas, and makes recommendations for improving the legal framework. The research questions center on whether the current legal framework is sufficient, if data collection businesses comply with privacy requirements, and what legal options consumers have when their data is compromised. The chapters of the study explore these important areas, including the evaluation of the legal framework, adherence to privacy laws when using big data, consumer protections and remedies, striking a balance between consent, informed consent, and the right to privacy, and the efficacy of legal interpretations of this right, with reference to "1984." The report highlights the pressing need for updated and modified laws to safeguard privacy and data security in the digital age. It emphasizes the significance of paying attention to the warnings in "1984" and the importance of privacy rights as basic human rights. The recommendations aim to strike a balance between individual liberties and technological advancement.

Keywords: *Phishing, Privacy, AI, Legal Framework.*

INTRODUCTION:

"Privacy is not something that I'm merely entitled to, it's an absolute prerequisite."

– Marlon Brando[1]

Data phishing has become a major threat in a period characterized by the rapid growth of artificial intelligence and the abundance of big data. In addition to causing worries about data insecurity, this phenomena also has legal ramifications, especially in light of the Information Technology Act of 2000. The present legal framework's protection of the fundamental right to privacy and data security is reminiscent of themes found in George Orwell's dystopian masterwork, "1984." This study examines the complex interactions between these components, illuminating the complex problems with data security and privacy in the era of artificial intelligence and big data while pointing out interesting parallels to George Orwell's terrifying picture of a surveillance state.[2]

Following are general targets of a phishing attack:[3]

1) Bank Account Number
2) Usernames and Passwords
3) Credit card details
4) Internet banking details

RESEARCH OBJECTIVES

- To evaluate the state of data phishing incidents today and the effects they have on customers in light of the development of AI technologies.
- To evaluate the Information Technology Act of 2000's protection of consumer rights

[1] Privacy is not something that I'm entitled to, it's an absolute prerequisite. — Marlon Brando : The Tribune India
[2] Vishwanath, A., Herath, T., Chen, R., Wang, J., Rao, H.R. Why do people get phished? Testing individual differences in phishing vulnerability within an integrated information processing model. Decision Support Systems, Vol. 51 No. 3, pp. 576-586. 2011
[3] Muhammet Baykara and Zahit Ziya Gurel, "Detection of Phishing Attacks," ISDFS, 2018

and its effectiveness in combating data phishing crimes.

- To determine and assess the difficulties and barriers that law enforcement organizations encounter when trying to identify and prosecute AI-driven data phishing cases in accordance with the Information Technology Act of 2000.

- To make suggestions and possible changes to the Information Technology Act of 2000 that might improve the law's applicability and efficacy in dealing with AI-related data phishing issues.

RESEARCH QUESTIONS

1. How well-suited is the current legal system—in particular, the Information Technology Act of 2000—to handle and prevent data phishing in the context of artificial intelligence and big data?

2. Whether businesses that gather and use big data are following privacy laws and guidelines, and if stronger enforcement measures are required.

3. Whether there are any gaps in the legal remedies available to consumers and whether they have enough protection and legal recourse in the event that their data is compromised or misused.

CHAPTERISATION

- **Chapter I:** In the context of AI and big data, the current legal framework—in particular, the Information Technology Act, 2000—is capable of effectively addressing and combating data phishing.

- **Chapter II:** Evaluating Big Data Collection and Use Compliance with Privacy Regulations and Calling for Stricter Enforcement.

- **Chapter III:** Assessing Consumer Protections and Remedies in Data Compromise and Misuse Cases - Finding Possible Loopholes.

- **Chapter IV:** In the Age of AI, Big Data, and Data Insecurity: Juggling Consent, Informed Choice, and the Right to Privacy.

- **Chapter V:** Orwell's "1984" is reflected upon as we evaluate how well legal interpretations of the right to privacy protect against ubiquitous surveillance and data harvesting.

Chapter I: In the context of AI and big data, the current legal framework—in particular, the Information Technology Act, 2000—is capable of effectively *addressing and combating data phishing.*

Data phishing, characterized by the deceptive acquisition of sensitive personal information, is on the rise. Cybercriminals employ increasingly sophisticated tactics, leveraging AI and big data to exploit vulnerabilities and manipulate unsuspecting victims. As a result, there are more data breaches, which can cause serious harm to one's reputation and finances.

Operation Phish Phry - Many bank customers reported experiencing data loss in 2009 as a result of giving sensitive information to fraudsters who then demanded their account number, login password, and credit card details. These forms seemed to have come from official websites, but they actually led users to fake ones. Approximately $1.5 million was stolen from hundreds of thousands of targeted bank accounts by the operation Phish Phry.[4]

In response to changing technological conditions, the Information Technology Act of 2000, which established the basic laws governing digital technology use in India, has undergone major revisions. However, the Act is confronted with new challenges, as it was conceived in a different technological landscape. Its adequacy in addressing the complexities of data phishing, particularly in the context of AI and big data, is a subject of considerable concern. This chapter meticulously evaluates key provisions of the Information Technology Act, 2000 that pertain to data security and cybercrimes. A critical examination of Sections 43, 66C, and 66D, among others, reveals the Act's limitations and its applicability to data phishing incidents involving AI-driven methods.

To underscore the gravity of the data phishing challenge, we present recent data breach statistics. These figures highlight the severity of the issue and the negative effects data breaches can have on one's finances and reputation, underscoring the need for the legal system to be sufficiently responsive to these kinds of events. According to the International Anti-Phishing

[4] https://www.phishprotection.com/blog/the-top-5-phishing-scams-in-history-what-you-need-to-know/

Work Group (APWG), phishing activity has skyrocketed in recent years, and more people are falling victim to phishing scams and attacks.[5] Despite the fact that many internet users are easily tricked by phishers due to their lack of awareness, it is hard to stay on top of the constantly evolving strategies employed by these criminals. Building efficient anti-phishing models is facilitated by machine learning techniques. This paper examines phishing as a classification problem and describes some of the latest intelligent machine learning methods that are employed as anti-phishing models in the literature, such as associative classifications, dynamic self-structuring neural networks, dynamic rule-induction, etc. This review aims to assist researchers, managers of organizations, computer security specialists, educators, and students who are interested in learning about phishing.[6]

Chapter II: Evaluating Big Data Collection and Use Compliance with Privacy Regulations and Calling for Stricter Enforcement

A thorough and in-depth analysis of privacy laws and their enforcement strategies is essential given the rapidly developing field of big data collection and utilization. This chapter advocates for the necessity of bolstering enforcement measures to protect individual privacy rights while navigating the complex complexities involved in ensuring compliance with privacy regulations within the context of big data.

Visual similarity based phishing detection

Visual similarity based phishing detection (VSBPD) monitors whether a user is giving away any kind of sensitive data to a suspicious web page. It keeps a check on the forms filled by the user, it looks for the similarities of text and images embedded on the page. It also stores user credentials and where they are to be sent. If the website is not on the trusted list, the processes is interrupted and a warning is generated. The warning is generally raised when there is similarity between two pages, in case both of them require the same information, however it is less likely for any of these websites to be fake if they are not similar in appearance. This

[5] Jain, K, Gupta, B. A novel approach to protect against phishing attacks at client side using auto- updated white-list. Security and Communications Networks. pp 1-20. 2017.
[6] Aburrous M., Hossain M., Dahal K.P. and Thabtah F. Experimental Case Studies for Investigating E- Banking Phishing Techniques and Attack Strategies. Journal of Cognitive Computation, Springer Verlag, 2 (3): 242-253. 2010.

approach is inspired by anti-phish (plug-in) and DOMAntiPhish (browser extension)[7]

The four Vs of big data—volume, velocity, variety, and veracity—define its pervasiveness in the current digital era. An era of transformation has begun as a result of the abundance of data; it is redefining organizations' operations, empowering decision-makers, and changing industries. However, this data revolution has also brought with it important ethical and legal considerations, particularly with regard to data privacy.

In response to these worries, governments throughout the world have passed data privacy laws and regulations, which are intended to safeguard individuals' private information and address the unique challenges posed by the big data era. Prominent legal frameworks such as the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR) of the European Union have set a significant standard for safeguarding privacy, with implications that impact enterprises globally. The aforementioned regulations prioritize the entitlements of individuals to exercise authority over their personal data, provide informed consent for its acquisition and utilization, and pursue redress in the event of any transgressions.

Nonetheless, there are difficulties in putting privacy laws into practice in the dynamic world of big data. Big data's intrinsic qualities, such as its enormous volume, diversity, and quick processing speed, can lead to complications that make compliance less effective. Moreover, the rapid advancement of AI-powered data analytics instruments poses supplementary difficulties, frequently surpassing regulatory advancements and requiring regulatory frameworks to be flexible.

To address these problems and ensure that privacy laws are properly implemented, stronger enforcement mechanisms must be put in place. Lax enforcement can lead to insufficient protection of personal information, which can erode people's trust in the digital ecosystem. It might lead to a sharp contrast between the harsh reality of data exploitation and the assurance of privacy protection, further undermining public trust.

Strict enforcement is vital, as evidenced by the recent spike in data breaches and privacy violations. Sensitive personal information has been made public in high-profile data breach

[7] Medvet, E., Kirda, E., & Kruegel, C. (2008). Visual-similarity- based phishing detection. In Proceedings of the 4th international conference on Security and privacy in communication networks, SecureComm ’08, Article no 2, pp. 1–11

cases, highlighting the necessity of enforcing laws and holding businesses responsible for data security. Organizations should place a high premium on upholding privacy laws and defending the rights of individuals to privacy. Serious consequences, such as hefty fines and legal ramifications, ought to follow violations of these regulations. A comprehensive approach is required to address the complex issues that arise at the intersection of big data and data privacy, so as to ensure that the benefits of technological advancement are balanced with the protection of fundamental rights.

Chapter III: Assessing Consumer Protections and Remedies in Data Compromise and Misuse Cases - Finding Possible Loopholes

The persistent and ever-growing threats of data compromise and misuse have a significant impact on individuals and organizations alike. Data breaches, improper use of personal data, and unauthorized access to personal information have become alarmingly commonplace. In addition to causing large financial losses, these incidents damage companies' and organizations' reputations and undermine the crucial trust that customers have in them.

This chapter provides a thorough analysis of the current legal safeguards intended to address the issues raised by data compromise and misuse, making it a crucial place to start. It performs a comprehensive analysis of relevant laws and rules, including notable statutes like the Information Technology Act of 2000, the California Consumer Privacy Act, and the General Data Protection Regulation (GDPR). A thorough understanding of the legal environment surrounding data compromise and misuse is attained by digging into the specifics of these frameworks. This paves the way for a more in-depth examination of any gaps and potential enhancements to the protection of personal information security and privacy.

Chapter IV: In the Age of AI, Big Data, and Data Insecurity: Juggling Consent, Informed Choice, and the Right to Privacy

The delicate balance between consent, informed choice, and the right to privacy has become increasingly important in the face of AI, Big Data, and data insecurity. The idea of consent is at a crossroads in a world where our personal data is continuously gathered, examined, and used to drive complex algorithms and artificial intelligence (AI) systems. Although consent is still the cornerstone of data privacy, there has been a paradigm shift brought about by the sheer volume and complexity of data transactions. People frequently encounter lengthy, intricate

privacy policies that are challenging to comprehend, let alone make wise decisions about. This casts doubt on the idea of "informed choice." Moreover, the constant threat of data insecurity, as demonstrated by the regular occurrence of data breaches, emphasizes how crucial it is to protect individuals' right to privacy. Striking the right balance between ensuring individuals have the autonomy to provide meaningful consent, promoting genuine informed choices, and upholding the fundamental right to privacy in an age of rapid technological advancement is a complex and evolving challenge. It calls for innovative legal and ethical frameworks that empower individuals while obligating organizations to enhance transparency, security, and accountability in the use of personal data, thereby mitigating the risks associated with the AI and Big Data era.

Chapter V: Orwell's "1984" is reflected upon as we evaluate how well legal interpretations of the right to privacy protect against ubiquitous surveillance and *data harvesting.*

A lesson in the possible erosion of individual privacy in the face of unbridled governmental power and intrusive technologies can be found in Orwell's dystopian vision of a totalitarian state where people are constantly monitored. Pervasive surveillance and data harvesting are no longer the exclusive domain of authoritarian governments; rather, they are now essential elements of contemporary democracies and corporate business models. It is the responsibility of legal interpretations of the right to privacy to lessen this intrusion on personal liberty and freedom. Yet in the face of changing practices and technologies, their effectiveness is becoming more and more strained. Even though many nations have laws and constitutions that protect privacy, the extensive use of data collection, algorithmic decision-making, and the international nature of data flows call into question how effective these legal measures are. The distinction between private and public life has become increasingly hazy in the era of widely used digital platforms and gadgets, which begs the question of whether the current legal systems are sufficient. Legal interpretations must change to reflect the complexity of contemporary surveillance and data harvesting, balancing national security concerns, technological advancement, and the protection of individual liberties in order to guarantee the right to privacy's continued relevance. Since the issues raised in "1984" are becoming more and more pressing in the realities of the twenty-first century, the legal landscape must change to reflect the shifting dynamics of our interconnected world.

CONCLUSION

In conclusion, the phenomenon known as "Data Phishing of Consumers" poses a significant challenge given the development of artificial intelligence, the decreased privacy of data resulting from data insecurity with big data, and the unprecedented access to personal information that companies have. This challenge touches on issues related to data security, privacy rights, and their social ramifications that are connected to the foresighted themes George Orwell explored in "1984." It also intersects with the legal framework established by the Information Technology Act, 2000.

The internet and artificial intelligence were not as commonplace as they are now, when the Information Technology Act of 2000 was conceived. The ever-evolving technological landscape and the highly skilled tactics employed by cybercriminals in data phishing incidents make it difficult for this legal framework to keep up. Its efficacy in protecting customers' privacy and data security in the AI-driven world is being investigated. This necessitates a thorough review of the Act, along with any necessary updates and revisions that can better handle the problems with data security and privacy today.

In George Orwell's dystopian novel "1984", citizens live in a surveillance state where their privacy is completely violated and they are continuously monitored. The novel serves as a sobering reminder of the possible repercussions of unrestricted data surveillance and loss of privacy, even though it is not a perfect parallel. The themes of surveillance and control depicted in "1984" become more timely in a time when governments have unprecedented access to surveillance tools and corporations gather vast amounts of data, frequently without the explicit consent of their citizens.

A fundamental human right, the right to privacy is protected by numerous international accords and is respected by many nations, including India. It is critical to understand that the Information Technology Act of 2000 should protect individual rights, such as the right to privacy, in addition to acting as a tool for technological regulation. Encouraging technological advancements while safeguarding citizens' data and privacy must be balanced by the Act. It must change to keep up with the rapidly evolving fields of artificial intelligence, big data, and data phishing. In a time when consumer trust is crucial and data has become a valuable asset, protecting data security and privacy is not only a legal but also an ethical and social issue. To

update the legal framework and put in place strong data protection measures, legislators, policymakers, and stakeholders must collaborate.

RECOMMENDATIONS

By bringing the Information Technology Act of 2000 into line with contemporary technological developments and the changing fields of artificial intelligence and data security, the proposed amendments seek to modernize the law. Recognizing the importance of data privacy, these changes include strict guidelines for data protection, breach notification, and non-compliance penalties. A comprehensive framework for data privacy highlights the dangers of unrestricted surveillance by emphasizing responsible data handling, modeled after Orwell's "1984". Companies will be required to obtain consent and provide accessible privacy policies if they are subject to transparency and informed consent requirements. Sensitive data will be protected by industry-specific cybersecurity standards and improved data security measures. Public awareness campaigns and strong regulatory agencies will deal with infractions and inform consumers about the risks associated with data privacy. Global data protection standards will be established through international cooperation, and ethical AI use places a focus on openness and responsible AI development. Data security and regulatory compliance will be further guaranteed by procedures for handling data breaches and frequent audits.