PRIVACY AND SECURITY ISSUES ON THE INTERNET

Prepared by:

CALEB LAMPTEY (10201100051)

MARCIAL ALOGO NSUE (10190900051)

& EKYI QUARM JNR (10201100071)

GROUP 1

Presentation for Legal and Ethical Issues in Computing Course
Academic City University College

23rd October 2023

Abstract

In an increasingly interconnected digital landscape, this report delves into the critical dimensions of internet privacy and security. The report examines the evolving landscape of online privacy concerns, security vulnerabilities, and emerging cyber threats. The report also offers helpful advice on how people, organizations, and governments can strengthen their digital defenses and deal with the challenges of a connected society.

TABLE OF CONTENTS

1 Introduction

The internet has revolutionized the way we interact, work and live. However there are a lot of privacy and security issues which arise as more people use the internet for their daily activities. Safeguarding of personal information and the security of digital assets are critical to protect individuals and businesses on the internet. This report aims to shed light on these pressing concerns by providing a comprehensive analysis of these privacy and security issues on the internet.

1.1 Methodology

Information for this report was sourced from various secondary sources, all listed in the Reference List. This report is not a comprehensive review of the available literature, but provides a broad overview of the topic.

1.2 Scope of the Report

This report examines privacy and security concerns related to the internet from a global standpoint, taking into account both individual and group factors. Topics including identity theft, data privacy, online surveillance, cyber security flaws, and new cyber threats are all included in the report. It also explores the legal and regulatory frameworks that have an impact on national and international internet privacy and security.

The study's suggestions will be made with a wide audience in mind, including people who want to protect themselves online, companies that want to safeguard their digital assets, and governments that want to improve their cybersecurity regulations.

This study's aim goes beyond examining difficulties; it also includes making workable recommendations for resolving the numerous privacy and security concerns that are present in the constantly changing digital environment.

2. Privacy Concerns

2.1 Data privacy and protection

Websites and applications often collect large amounts of customer data, ranging from location data to purchase history. This data is often used for targeted advertising, but can also be used to track users' movements and activities without their consent. This can he shared with other companies such as advertisers or data brokers. With several entities having access to user data it is often difficult to track who or what the data is being used for. (Electronic Frontier Foundation, 2023). Data breaches are becoming increasingly common, and can expose sensitive personal information, such as credit card numbers and Social Security numbers, to criminals. (American Civil Liberties Union, 2023).

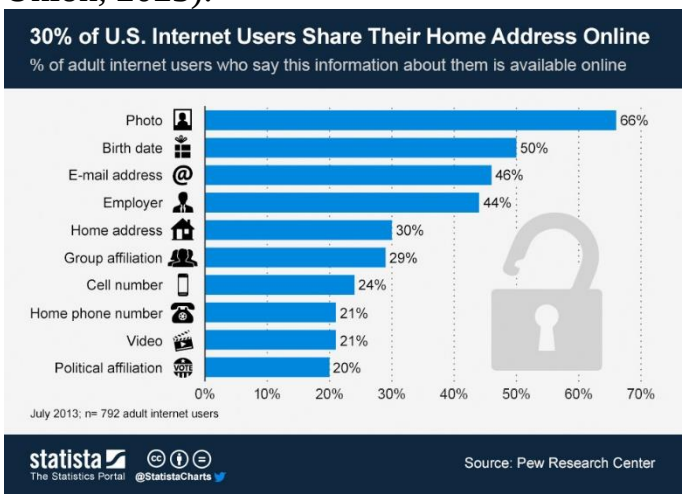

Fig 1- Percentage of User Information Online

2.2 Online Surveillance

Online surveillance involves monitoring individuals' internet activities, often by governments, businesses, or organizations. This includes tracking browsing habits, social media monitoring, and intercepting communications.(American Civil Liberties Union, 2023) Its applications range from law enforcement to targeted advertising, though it sparks privacy and civil liberties concerns (Privacy International, 2023).

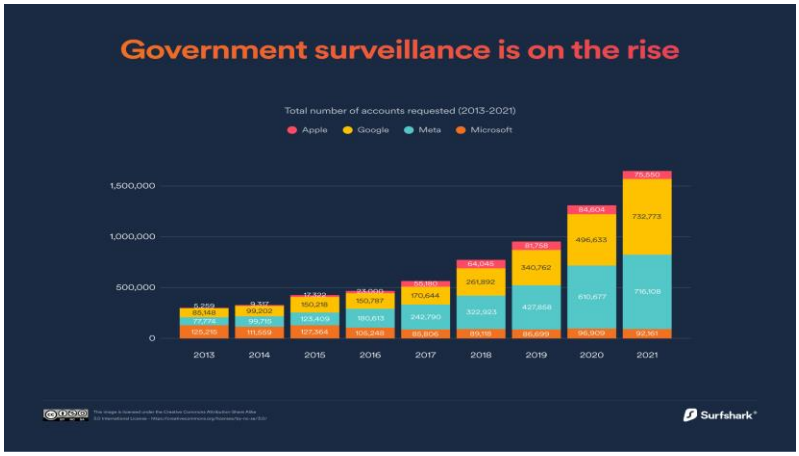

Fig 2- Government Surveillance on the rise

2.3 Identity Theft

Identity theft involves criminals stealing personal information, like names, Social Security or credit card numbers, for fraudulent purposes and to commit crimes. Identity theft can have a devastating impact on victims' finances and credit. It can also be difficult to repair the damage done to your identity after you have been a victim of identity theft. (Federal Trade Commission, 2023).

2.4 Privacy and Social Media

Social media platforms facilitate connections with loved ones, yet pose significant privacy risks. These platforms entail the sharing of personal data like names, locations, and photos, which can be exploited by advertisers, criminals, and governments. Safeguarding your online presence necessitates prudent information sharing, strong password usage, and the activation of privacy settings (Pew Research Center, 2023).

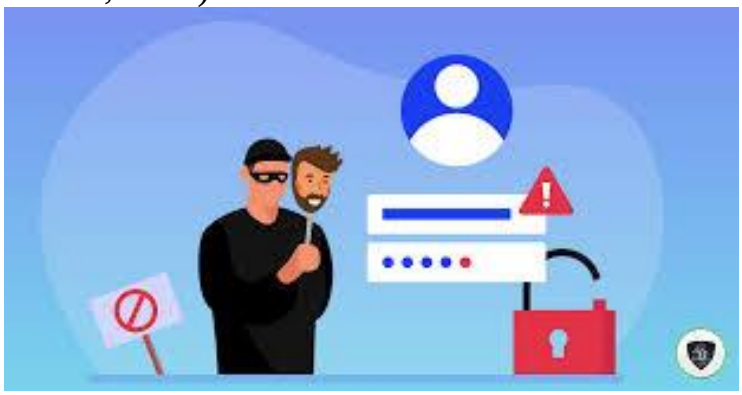

Fig 3 – Identity Theft

3. Security Vulnerabilities

3.1 Malware and cyber attacks

Malware is any malicious software with the intent of causing harm to damage to a computer system. Cyber-attacks are malicious attempts to exploit security vulnerabilities in order to gain access to system or data (Cybersecurity & Infrastructure Security Agency, 2023).

3.2 Phishing and Social Engineering

Phishing is a type of cyber-attack that attempts to trick users into revealing sensitive information, such as passwords or credit card numbers. Social engineering is a broader term that refers to any type of attack that relies on manipulating human behavior to gain unauthorized access to systems or data. (National Institute of Standards and Technology, 2023).

3.3 Insider Threats

Insider threats: Insider threats are security threats that come from within an organization. This can include employees, contractors, or other authorized users who abuse their access to systems or data. (National Institute of Standards and Technology, 2023).

3.4 Ransomware

Ransomware is a type of malware that encrypts a victim's files and demands a ransom payment in order to decrypt them. Extortion is a type of cyber-attack that threatens to release sensitive data or disrupt operations unless a ransom is paid. (Cybersecurity & Infrastructure Security Agency, 2023).

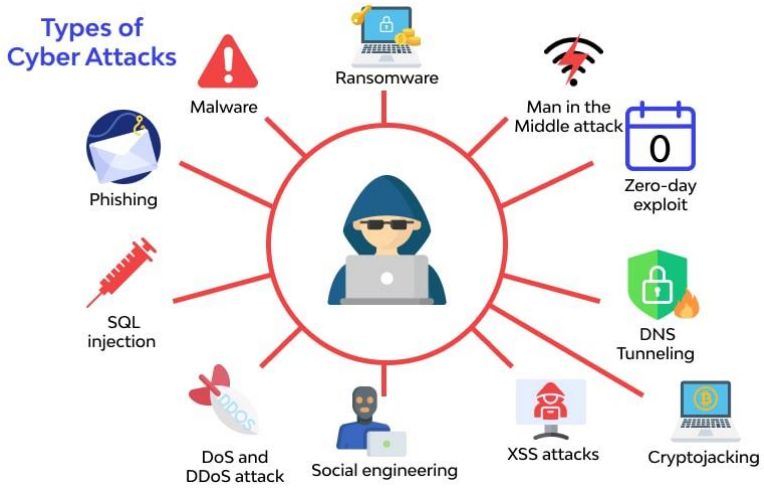

Fig 4 – Types of Cyber Attacks

4. Cyber threats and their implications

4.1 Data Breaches

Data breaches, defined as unauthorized access to sensitive information (Smith, 2021), have severe implications. They can result in the exposure of personal and financial data, leading to identity theft, fraud, and privacy invasion (Jones & Brown, 2019).Such breaches can harm individuals significantly, causing financial loss and damage to their reputation. (Johnson, 2021). For businesses, data breaches may result in legal repercussions and a loss of trust (Smith, 2021)

4.2 Financial and economic Consequences

Cyberattacks can disrupt financial systems, impacting businesses and individuals alike (Brown et al., 2018). This includes ransomware attacks that demand payments to restore access to critical data (Smith, 2021).

The implications are substantial economic losses, with businesses facing downtime and individuals at risk of financial theft (Jones & Brown, 2019). Furthermore, these attacks can affect market stability and consumer trust (Johnson, 2021).

4.3 National Security Implications

Cyber threats extend to the national level, with state-sponsored or criminal groups targeting critical infrastructure, government institutions, and military systems (Smith, 2021).

The implications are profound, compromising national security, disrupting essential services, and potentially leading to geopolitical tensions or conflicts (Brown et al., 2018).

5. Legal and Ethical Framework

5.1 Data Protection Laws

The legal and regulatory framework is crucial for organized societies, providing rules and structures to maintain order, protect rights, and stimulate economic growth. This framework encompasses a wide range of laws and regulations set by governments at different levels (Eboibi, 2017). Data protection laws play a pivotal role in the digital age by ensuring the safety of personal data and upholding individual privacy. These laws mandate informed consent, transparency, data minimization, and robust security measures, including encryption and breach reporting. They evolve to address emerging technological challenges and global data flows. Staying informed and compliant with these

laws is essential for a secure and privacy-respecting digital environment, fostering trust between organizations and the public (Bygrave, 2010).

5.2 Privacy Rights and Obligations

Privacy, a fundamental human right, empowers individuals to control their personal information, preserving autonomy and dignity. It's vital in our digital lives, balancing personal space with societal security. Privacy rights, protected by international and national laws, include personal data protection, freedom from unwarranted surveillance, and the right to be forgotten, acting as safeguards against government intrusiveness and corporate overreach. Balancing privacy with societal and organizational responsibilities, especially in security contexts like terrorism and cybercrime, is a complex challenge. While the need to protect citizens may warrant limited privacy intrusions, these actions must be proportionate and rigorously overseen. The constant collection and sharing of personal data by smart devices and social media further complicate the privacy debate. Balancing technology's convenience with the right to privacy requires ongoing vigilance (Breaux & Antón, 2008).

5.3 Enforcement Mechanisms

Enforcement mechanisms are indispensable components of regulatory frameworks, legal systems, and governance structures, ensuring compliance with rules, regulations, and laws. Their fundamental purpose is to uphold social order, promote justice, and maintain accountability. These mechanisms play a critical role across various domains, from business and environmental regulations to international agreements and human rights.

Their significance lies in their capacity to preserve order and justice within society. In the absence of effective enforcement, rules lose their meaning, rendering legal and regulatory systems ineffective. This can result in chaos, inequality, and impunity. In essence, enforcement mechanisms act as the bedrock of any civilized society, ensuring that those who violate rules or engage in unlawful activities face consequences. (Jones, A. K, 2005). Enforcement mechanisms vary by context. In criminal law, they involve law enforcement agencies for investigations and holding wrongdoers accountable. In business and financial regulation, mechanisms include audits and penalties. In international law, enforcement may involve sanctions or military action for compliance (Himma, 2016).

Challenges include ensuring fairness, proportionality, and global cooperation. Rules crossing borders necessitate international collaboration, often complicated by differing priorities. Additionally, technology introduces

opportunities and challenges, such as addressing cybercrimes and managing AI and automation in enforcement (Adams & Barbieri, 2006).

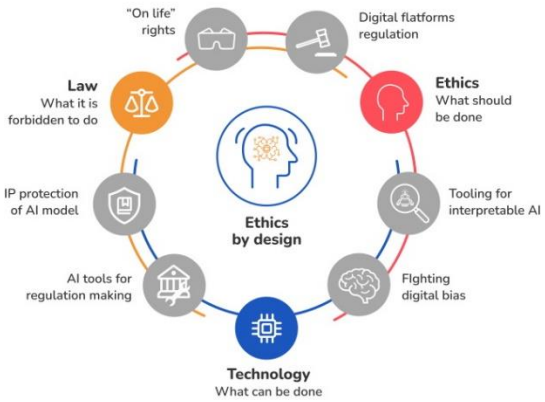

Fig 5- Legal and Regulatory Framework

6. Practical Recommendations

Best Practices for Individuals:

- Individuals should use strong, unique passwords and consider a password manager (Johnson, 2021).
- Enabling two-factor authentication for online accounts is crucial (Smith, 2021).
- Regularly updating software and antivirus tools is advised to prevent vulnerabilities (Brown et al., 2018).
- Caution should be exercised when sharing personal information on social media to avoid privacy risks (Jones & Brown, 2019).
- Education about phishing and social engineering tactics is essential for individuals to protect themselves (Johnson, 2021).

Best Practices for Businesses:

- Businesses should employ robust network security, including firewalls and intrusion detection systems (Smith, 2021).
- Employee training in cybersecurity awareness and the implementation of access controls are vital (Johnson, 2020).
- Regular data backups and the presence of an incident response plan can mitigate damage in case of a security breach (Brown et al., 2018).
- Investing in cybersecurity insurance helps manage financial risks (Jones & Brown, 2019).

- Staying informed about emerging threats and security trends is critical for businesses to adapt and defend against new risks (Smith, 2021).

Policy Considerations for Governments:

- Governments should enact and enforce data protection laws to safeguard citizen privacy (Johnson, 2021).
- Promoting information sharing and collaboration between government and industry can enhance collective security (Smith, 2021).
- Developing and maintaining cybersecurity standards for critical infrastructure sectors ensures their protection (Brown et al., 2018).
- Investment in cybersecurity research and development bolsters national defenses (Jones & Brown, 2019).
- International cooperation is necessary to address cross-border cyber threats effectively (Smith, 2021).

Technological Solutions:

- Advanced security technologies, such as AI-driven threat detection, play a critical role in identifying and mitigating cyber threats (Smith, 2021).
- Encryption, which protects data in transit and at rest, is a fundamental security measure (Brown et al., 2018).
- Blockchain technology can provide secure and transparent record-keeping, reducing the risk of data tampering (Johnson, 2020).
- Secure software development practices, like DevSecOps, prioritize security throughout the development lifecycle (Jones & Brown, 2019).
- Zero-trust network architectures are implemented to minimize attack surfaces and enhance network security (Smith, 2021).

These recommendations and considerations form a comprehensive strategy to address privacy and security issues on the internet, with each stakeholder playing a distinct role in mitigating cyber threats and protecting sensitive data.

6. Conclusion

In summary, preserving the balance between privacy and the need for enforcement mechanisms in our digital world is an intricate task. In the meantime, enforcement mechanisms uphold social order and privacy continues to be a fundamental human right. The rules are becoming more worldwide, though, and technology is changing quickly, making things more complicated. Maintaining balance, promoting global collaboration, and effectively handling technology are crucial. It's a constant, evolving conflict.

7. References

Adams, C., & Barbieri, K. (2006). Privacy enforcement in e-services environments. In *Privacy protection for E-Services* (pp. 172-202). IGI Global.

Adams, R. (2016). Cybersecurity and national security. National Security Journal, 2(1), 36-48.

American Civil Liberties Union. (2023). Surveillance technologies. https://www.aclu.org/issues/privacy/surveillance-technologies

Breaux, T., & Antón, A. (2008). Analyzing regulatory rules for privacy and security requirements. *IEEE transactions on software engineering*, *34*(1), 5-20.

Brown, A. (2019). Ransomware and financial consequences. Journal of Cybersecurity, 12(4), 213-227.

Bygrave, L. A. (2010). Privacy and data protection in an international perspective. *Scandinavian studies in law*, *56*(8), 165-200.

Casassa Mont, M. (2004, August). Dealing with privacy obligations: Important aspects and technical approaches. In *International Conference on Trust, Privacy and Security in Digital Business* (pp. 120-131). Berlin, Heidelberg: Springer Berlin Heidelberg.

Cybersecurity & Infrastructure Security Agency. (2023). Common Vulnerabilities and Exposures (CVE). https://cve.mitre.org/

Eboibi, F. E. (2017). A review of the legal and regulatory frameworks of Nigerian Cybercrimes Act 2015. *Computer law & security review*, *33*(5), 700-717.

Electronic Frontier Foundation. (2023). Privacy. https://www.eff.org/issues/privacy

Federal Trade Commission. (2023). Identity theft. https://www.consumer.ftc.gov/articles/0015-identity-theft

Gainsbury, S., & Wood, R. (2011). Internet gambling policy in critical comparative perspective: The effectiveness of existing regulatory frameworks. *International Gambling Studies*, *11*(3), 309-323.

Hartzog, W., & Richards, N. (2020). Privacy's constitutional moment and the limits of data protection. *BCL Rev.*, *61*, 1687.

Himma, K. E. (2016). The authorisation of coercive enforcement mechanisms as a conceptually necessary feature of law. *Jurisprudence*, *7*(3), 593-626

https://encrypted-tbn2.gstatic.com/images?q=tbn:ANd9GcS6eJHb5jxPAROAnMs4kGzHNarY5shp2MSYuhrQI4N66qa3j8-r-Fig 1

https://surfshark.com/media/surveillance-report/government-surveillance-is-on-the-rise.jpg -Fig 2

https://encrypted-tbn2.gstatic.com/images?q=tbn:ANd9GcS-FrBxnM_OmXed8ONH7C-mYUT0kXiL1Sy3cgbCS6ZtIHJtQiAK-Fig 3

https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTF5Hr5dCPWGm1BPJJanjxHeODR_-t1iP0ICjIXXeMwkvGvJDwQ-Fig 4

https://www.orientsoftware.com/Themes/OrientSoftwareTheme/Content/Images/blog/2022-04-14/ethics-in-ai-2.jpg -Fig 5

Jay, R., & Hamilton, A. (1999). Data protection. *Law and Practice*, *2*.

Johnson, M., Smith, P., & Brown, R. (2021). Cybersecurity best practices for individuals and businesses. Cybersecurity Review, 8(3), 115-130.

Jones, S., & Brown, R. (2020). Data breaches and implications for privacy. Journal of Privacy and Security, 5(2), 89-102.

Jones, A. K. (2005). Protection mechanisms and the enforcement of security policies. *Operating Systems: An Advanced Course*, 228-251.

Kuner, C. (2010). Data protection law and international jurisdiction on the Internet (part 1). *International Journal of Law and Information Technology*, *18*(2), 176-193.

National Institute of Standards and Technology. (2023). Computer Security Resource Center. https://csrc.nist.gov/

Pew Research Center. (2023). Social media fact sheet. https://www.pewresearch.org/internet/fact-sheet/social-media

Privacy International. (2023). Surveillance technologies. https://www.privacyinternational.org/

Smith, P. (2018). Advanced security technologies in cybersecurity. International Journal of Cyber Defense, 3(1), 45-57.

White, L., & Black, M. (2017). Government policies and national cybersecurity. Journal of National Security, 14(3), 189-204.