How to Cite:
Meshram, S. (2022). Privacy intrusion: Reasons and consequences. *International Journal of Health Sciences*, *6*(S6), 6475–6485. https://doi.org/10.53730/ijhs.v6nS6.11106

Privacy intrusion: Reasons and consequences

Ms. Shruti Meshram
Postgraduate Institute of Business Management, Sardar Patel University, Vallabh Vidyanagar, Gujarat, India

Abstract---Given the dynamic nature of the online sphere, means of privacy intrusion and issues are changing rapidly. The literature review provides insight into the entities affected such as individuals, organizations, and Governments. An exploratory study is being conducted to discuss the current scenario for various privacy intrusion mechanisms, relevant regulations, and their severe effects on individuals. The tales of privacy intrusion generates privacy concerns among individuals and demand privacy protection policies and regulations by the Government. The study evolutes around a deep understanding of the reasons for privacy intrusion, its' current scenario, and its consequences for the same. The perception of misuse of technology is severely felt by the entity suffering individuals. Policymakers should heed attention to the factors which are invisible to logic and reasoning but have an insidious impact on individuals, groups, and society (Dinev et al., 2015). Privacy study is helpful for sociologists, psychologists, scholars of communications, management, information, organizational behavior, law and regulation, and public policy. The study also helps to build the judicial framework for the preparation of concurrent relevant privacy policies.

Keywords---privacy, privacy intrusion, government regulation, privacy concern.

Introduction

Privacy is one of the most evolved concepts of human society. Men from the stone age have evolved the concept of isolation via residing in an enclosed area for safety and private wellbeing and formulated society for mental upkeeping. This differentiation between individuals and society uplifted the sense of privacy even to a greater extent for different social norms. So privacy is a socially created need (Dinev, 2014).

Privacy is defined as: *The need for privacy has evolved as protection against disclosure of damaging mistakes, bruising, and disapproved contacts*
- (Westin, 1967)

Privacy is the right to be left alone, or freedom from interference or intrusion (Warren & Brandeis, 2005). Physical privacy is defined by tangible boundaries such as gated mansions, tented windows, etcetera. With the advent of electronic gadgets, privacy is extended from physical privacy to information privacy due to its reachability beyond physical boundaries and is anonymously referred to as information or data privacy. Adherence to physical privacy is a form of social norms and so hard to break due to individuals' cautious social behavior. Nowadays the use of technology is omni present for physical as well as for information privacy intrusion. Cyberworlds do not possess any visual boundaries to distinguish the level of privacy available. It is easy to break the privacy boundaries in cyberspace with the help of IP addresses and cookies (Regan, 2002). Physical privacy intrusion has been cannibalized by the information privacy intrusion with the advancement of various electronic gadgets and information technology. This merging of physical and information boundaries is considered the pervasive dissolution of boundaries by some scholars whereas other scholars consider it as an absence of intention to segregate these boundaries (Jeff Smith et al., 2011a).

Information privacy is defined as: *the number of control individuals can exert over the type of information, and the extent of that information revealed to others*. (Westin, 1968)

Privacy norms differ with the level of societal development. Ethically and morally advanced societies show higher privacy norms with stronger value systems. Privacy depends on a sense of judgment with a clear understanding of what's wrong and what's right. This sense of judgment evolves with the social fabric with strong individual self-credence and well-developed competitiveness, and sturdy religious beliefs and customs (Dinev, 2014). Basic human values are vague and ill-defined. Privacy invasion is an insult to individuality and human dignity. The necessity of legal protection for privacy intrusion itself put human dignity in question (Sipior et al., 2004). Definitions available for privacy and its intrusion are time-specific. *Privacy, however, is a concept in disarray. Nobody can articulate what it means* (Solove, 2008). This impales us to think about it loudly and clearly. Tamara Dinev feels that the people, organizations, and government's perception of privacy differs and many a time ambiguous, and paradoxical. Due to widely spread electronic usage and the world wide web people are unable to understand how to protect themselves from any kind of privacy intrusion and data collection. They either are not aware of the degree and extent of data collection by different entities or they are unable to protect themselves through any mechanism.

The "state of nature" or the law of nature that being all equal and independent, no one ought to harm another in his life, liberty, and property (Jos, 2006).

The intention of harming others itself constitutes an ethical issue. Privacy intrusion is such an issue to demand legal protection. If privacy is not protected, intrusion possess a bigger threat to individuals and societies. Privacy and its intrusion require clearly defined terms for its understanding. We also require procedures and guidelines for protection from intrusion. If privacy is intruded upon, it generates various severe psychological and physical consequences. In the

absence of clear guidelines about the identification, notification, and awareness, the reporting of such offenses is not happening at even a moderate rate. With the advent of technology, privacy intrusion is blooming at a haphazard rate. Between January 1, 2005, and May 31, 2020, there have been 11,762 recorded breaches (Sobers, 2021). At present, the global annual cost of cybercrime is estimated to be $6 trillion per year which is estimated to reach $10.5 trillion annually by 2025 (Purplesec, 2021). Privacy intrusion is a judiciously punishable offense in a few countries and there is a rare chance of escape of the offender(s)/culprit(s) in the presence of better aware societies and stronger judicial systems.

Literature review

Invasion of privacy occurs when a person or entity intrudes upon the personal lives of others without just cause. Intrusion is defined as disturbing an individual's tranquility or solitude (Solove, 2008). Fragments of privacy can be segregated by various prominent scholars separately. Pedersen (1997) described the fragments of privacy as solitude, isolation, anonymity, reserve, intimacy with friends, and family. Solitude places a person to be undisturbed by others or places the self in a situation where they are unseen or unheard, or the right to protect individual dignity of private activities, or an individual intrudes upon another person's private affairs in a physical manner such as intercepting phone calls, peeping, taking photographs without the victim's knowledge or consent, video recording the victim in his or her home without consent or knowledge. Reserve is controlling verbal disclosure of personal information to others. Isolation means keeping physical distance to separate oneself from others. Intimacy with family and friend/s states to being alone with the members of the family and friends. Anonymity means privacy by going unnoticed in a crowd of strangers. These fragments of privacy are again aligned with the privacy functions provided by westing in 1967. Clark and Westin (1968) demarcated privacy as Solitude (freedom from observation by others), Intimacy (being alone with others, such as friends and family), Anonymity (being unnoticed among others), and Reserve (unwillingness to disclose personal information to others).

Privacy is also defined differently by Jeff Smith et al. (2011b). They perceive and define the terms 'what is not the privacy' which consists of overlying concepts such as anonymity, confidentiality, security, and secrecy. Anonymity is defined as individuals limiting the availability of identifiers to others, confidentiality talks of controlling the disclosure of the information, ethics is the responsibility to engage in the moral conduct regarding privacy, and secrecy is the intentional concealment of information. Security is the protection of personal information with integrity (information is not altered during transit and storage), authentication (verification of a user's identity and eligibility for data access), and confidentiality (data use is confined to authorized purposes by authorized people). Privacy could be contextual. Context-specific information can be the domain (discipline), the rationale (why), occupation (who), time (when), location (where), and culture (with whom) oriented (Bansal et al., 2016). Privacy either depends on or derives from the nature of its threats (Jeff Smith et al., 2011a; Smith, 2011). Van Aaken et al. (2014) argue that privacy should be perceived as a specific form of freedom and individual freedom should be prioritized over any other value.

Term Information/data privacy originated from the introduction of different uses of technology in daily life utilizing various electronic gadgets. These gadgets help intruders to steal individual personal data. These gadgets could be offline or online and are the reasons for concern for the individuals. Offline, privacy intrusion is possible with unauthorized/authorized surveillance with the gadgets like CCTV which are cabled to the center point or server. Recently online mode of these surveillance mechanisms is also been used. Online privacy intrusion occurs with the predominant use of the Internet. Internet privacy abuse is categorized either as harmless abuse (targeted on marketing stunt) or malicious abuse (identity theft and social engineering to get details of individuals for malicious purposes) (Alimatu-Saadia Yussiff, Abdul-Lateef Yussiff, 2013). A few of the latest privacy intrusion technologies are whole-body imaging scanners, RFID-enabled travel documents, unmanned aircraft systems (drones), second-generation DNA sequencing, human enhancement technologies, and second-generation biometrics (Finn et al., 2013). New technologies such as remote mind/brain reading/listening are flourishing in recent times (Harsha Vardhini & Deepthi, 2017).

The evolution of different electronic gadgets and technologies such as sensors, wireless communications, automatic identification and tracking, distributed services, broadband Internet access, and embedded computing has shown us the way to use these smart objects via the Internet for daily affairs. These technologies also provide means for privacy intrusion (Zarpelão et al., 2017). National identification cards and biometrics (electronic identification technology) using fingerprint, geometry, voice, facial scanners, retinal, iris and hand thermal) are other forms of privacy intrusion.

"*privacy often is privileged over the common good,*" - (Cheng, 2016).

Privacy intrusion is being defined differently by different individuals and social entities or groups. Privacy intrusion results in privacy concerns. Privacy concerns are categorized as 'freedom from intrusion', 'negotiating the public/private divide', 'identity management and 'surveillance'. One example of this type of privacy is 'Freedom from intrusion'. Home is the place where any kind of privacy intrusion is considered unconstitutional by the US supreme court with the statement as

'In the home, all details are intimate details [and] the entire area is held safe from prying government eyes.

The bigger questions on the horizon are whether the individuals, groups, and societies possess the right to privacy from the governing body using proper regulations; are those entities free from any type of privacy intrusion; and whether in the case of intrusion the judicial system is actively in place to punish such offenders? To search for the answers to the above questions an exploratory study has been conducted.

Research Methodology

Research design is exploratory research for this study. Secondary data is used as the foundation to appraise the study's purposes critically. Research articles

/papers from various journals of repute are being used for the study. Various websites are being used for the literature review. The literature review resulted in the following research questions:

- What are the probable reasons for privacy intrusion?
- What is the current scenario for privacy intrusion?
- What are the consequences of privacy intrusion?

Data Analysis and Discussion

Technology can prove to be a blessing or menace depending upon use. The very basic objective of the safety of individuals with the help of electronic gadgets turned into a curse through privacy intrusion. Three entities are strongly affected by privacy intrusion: individuals, organizations, and government. (i) Individuals develop privacy concerns. (ii) Organizations (a firm or a website) develop two different points of view. The first view talks about privacy notices which are prepared by experts in law and communications for the legal implications. The second view talks about practices that rest on the organization–customer relationships. These practices ask for fair procedures for handling customers' personal information. (iii) The government should enforce legal protection to individuals through privacy policies and regulations. Government regulations should balance organization-self-regulations as well (Ginosar & Ariel, 2017).

Information privacy could be understood with the help of the contributing factors such as user privacy awareness for data collection, errors in the information, secondary use of information, privacy control, and unauthorized use of information. Organizations foster individuals' perceptions of control over their personal information by providing privacy control with error-correcting rights. Such privacy control seems to be superficial as individuals fear other factors are as intrusive as well. With the unmatched or unparallel rate of technological up-gradation privacy awareness always seems to be in question for the population. To gain individual trust organizations upgrade their privacy protection technological setup and announce self-policing associations with individuals. Individuals can protect personal data with the help of secure cookies. Secure cookies offer security by removing individual databases per machine shut down (Park & Sandhu, 2000). Alongside proactive individual privacy awareness, there is a need for a strong reactive judiciary system. A good judiciary system restrains the organizations to act in opportunistic behavior (Xu et al., 2012). It is equally true for government surveillance.

Reasons for privacy intrusion

The probable reasons for privacy intrusions are power gained over others for personal advantage such as financial gain, health and fitness perspective, physical abuse, character assassination, intellectual submission etcetera. Individuals, organizations, and government are equally responsible for privacy intrusion. In most cases, reasons for privacy intrusion by individuals are gender-specific physical, and psychological abuse through camera-specific stalking. Individuals suffer harassment via the Internet specifically females (one in every six females) as compared to males (one in every 19 Male) (Jovanovic, 2022).

Reasons for privacy intrusion by organizations are monetary gain and business expansion. This privacy intrusion by the organization is happening through cookies which are sent to user/individual machines (desktop/laptop etcetera) to gather personal data. In exchange, organizations provide compulsory comfort of customized Internet surfing experience to the individuals as in most of the cases there is non-availability of opt-out option for the notice of the use of cookies provided by organizations or websites.

The reason for privacy intrusion by the government is the power gained over others via surveillance to get personal information. The form of personal information collected could be taxation as well as financial information, marital status, water use, electricity, registrations of cars, residency, political affiliations, electoral success etcetera. Along with these mechanisms to gather individual information, Government also uses phone taping and satellite surveillance to monitor individual(s) activities for political and defense reasons. Such type of pestering induces terror, fear etcetera among individual to be blackmailed by the intruder.

Current scenario of privacy intrusion

Information privacy intrusion can be understood with the help of different cases of cyber breaches. Global cyber breaches suffered an annual cost of $6 trillion in 2022. The average cost of a data breach has increased by $137,000 due to remote work during Covid 19. Privacy breaches enlisted extortion, identity theft, personal data breach, non-payment, and phishing attacks in 2021 (Purplesec, 2021). The most common methods for cyber breaches are phishing/ spear-phishing, DDoS attacks, SQL injection attacks, rootkit, and malware like adware, Trojan horse, and spyware. The amalgamation of electronic gadgets and information technology resulted in different remote privacy intrusion mechanisms such as mind-reading via satellite link etcetera. According to the survey of American citizens, 86% of breaches were financially motivated against 10% for espionage. Human error contributes to 95% of cybersecurity breaches. In the case of data breaches, individuals have no idea about reactive action. It is felt that cyber security jobs are difficult to fill as there is a lack of availability of qualified professionals (Sobers, 2021).

Digital footprints are the key to any type of privacy intrusion which leads to cybercrime. The rate of Cyberattacks is 39 seconds per attack. According to one survey conducted by Pew Research Center, Government is the least trusted entity by 64% of Americans. Reading privacy policy is not a trend till now. 39% of Americans are ready to give up their most preferred activity for one year in the exchange for better online security. These statistics are provided by 'The National Center for Victims of Crime' (Jovanovic, 2022). Privacy intrusion is a punishable offense for the culprit under common law (Cveticanin, 2021). Music, movies, software, and books are subject to piracy. Piracy in India stands third with 9.589 billion illegal visits (Spajic, 2021). A proactive cybersecurity incident response plan is a need of the hour (TitanFile, 2022). Protection of privacy is seen as a constitutional right in USA judicial system. Invasion of privacy is aligned with the civil rights violation. Such types of offenses are addressed in civil court proceedings. (Clark & Westin, 1968; Westin, n.d.). The organization for Economic

Cooperation and Development (OECD) drafted Fair information practices (FIP) in the year 1980. This FIP consists of five principles as notice (transparency), choice, access (Information review and correction), security/Integrity (Information protection), and enforcement/redress (accountability) (IAPP, 2007; Spake et al., 2011).

In Europe, privacy is viewed as a 'human rights issue (Dinev et al., 2015). In European countries, privacy is regarded as a fundamental right protected in many international and national constitutions. European Convention of Human Rights offers a right to 'respect for privacy and family life (Article 8) (Dinev, 2014). European Data Protection Supervisor and 'General Data Protection Regulation' GDPR are the privacy protection law enforcement bodies. As per the European Convention on Human Rights, contributing factors for privacy protection need to be part of the national constitutions of the EU Member States and the Charter of Fundamental Rights of the European Union. 'Right to privacy' forms a foundation for the European Member States' data protection legislation (Weber, 2015). Based on FIP principles GDPR is formed by European Union. GDPR is a regulatory body enforced on 25 May 2018. GDPR is directly binding and applicable with flexibility for individual state-specific implementation. Many countries adopted and developed location-specific enforceable regulations. For example - The California Consumer Privacy Act (CCPA), based on similar principles is adopted on 28 June 2018.

Some countries have adopted the principles of GDPR into their administrations but few the countries still need to heed attention to such activities and enforce an appropriate law. The Constitution of India provides privacy protections to individuals through the 'right to privacy' for their online data, and violations of the same. Given the dynamic nature of the online sphere, privacy concerns and issues are changing rapidly, and keeping pace with such developments is a tough task. The pertinent laws in India dealing with data protection are the Information Technology Act, 2000, and the (Indian) Contract Act, 1872 for the punishment for privacy intrusion. These acts are lacking the pace with current upgrades on the technical front and need to be amended with concurrent development in the field of electronic and information technology.

Consequences of privacy intrusion

Over time, information privacy intrusion gradually results in privacy concerns. Privacy concerns have increased gradually with a very large pool of 'data loss' events from 2000 onwards. Individuals depict more privacy intrusion for personalization of browsing experiences (Antón et al., 2010) by organizations. The consequences of privacy intrusion are various psychological and physical problems in individuals. These can be categorized as fear, helplessness, irritation, insecurity, depression, frustration, insecurity, avoidance, unhappiness, sadness, an attitude of indifference etcetera. Many prominent researchers in the field have conducted research regarding the same as follows: Tamara Dinev (2008) affirms that surveillance has a social cost and psychological effects on individuals if monitored. One paper "Employee Stress and Health Complaints in Jobs With and Without Electronic Performance Monitoring," mentions one experiment conducted by Smith. It is found that electronically monitored workers contribute to a lower

level of productivity alongside other psychological effects such as depression, anxiety, and tension even though it does not constitute monitoring private affairs.

Tamara Dinev in her paper "Internet Users' Beliefs about Government Surveillance – The Role of Social Awareness and Internet Literacy" explains the role of social awareness and Internet literacy in post-9/11 American society. Her findings are: (i) American people believe higher Internet literacy plays a crucial role in understanding the government's role in privacy intrusion concerns. With higher Internet literacy people despise government surveillance and perceive it to be an unwanted privacy intrusion. (ii) This finding is again supported by another relationship between 'Internet literacy' and 'need for the government surveillance' which narrates the same tale of higher 'Internet literacy' level people don't find the idea of 'government surveillance' favorable (Dinev, 2008). In one study 'Privacy Indexes: A Survey of Westin's Studies' by Kumaraguru & Cranor (2005) relevance of the privacy index created by Westin was studied in detail. Westin has done 30 studies to understand privacy in detail. He has created privacy indexes to understand the privacy trend from 1978 to 2004. He had created various privacy indexes such as General Privacy Concern Index, Consumer Privacy Concern Index, Medical Sensitivity Index, Medical Privacy Concern Index, Consumer Fear Index, Distrust Index, Privacy Concern Index, Privacy Segmentation Index, and Core Privacy Orientation Index. Westin has categorized the respondents as the privacy fundamentalists (25%), the Pragmatic (57%), and the Unconcerned (18%) and drawn conclusion that the population has gained a higher privacy concern index over time from 31% in 1978 to 56% in 1998

Various privacy studies affirm that privacy intrusion occurs in different ways. King & Chen (2003) in their study elaborate on the procedure for backtracking the online privacy intrusion. This backtracking of privacy intrusion is a great help in identifying the real culprit for the offense and rendering appropriate punishment. Such types of privacy intrusion offenses require good law and order inside the country and a great judicial system in place. One of the consequences of privacy intrusion is: that there is a need for Government regulations. The government provides rules and regulations as a matter of privacy protection policies to gain individual trust and protect individuals from unauthorized use by politicians for power gain. Various countries have privacy protection right embedded in their constitution and strong judicial system with frequent amendments aligned with concurrent technological upgrades. Individuals, as well as organizations, need to ensure critical infrastructure, use of valid computer applications, network security, cloud security, and IoT (Internet of Things) security for protection against cybercrimes (Jovanovic, 2022).

Conclusion

There is a need for defining terms for privacy and privacy intrusion. The tales of privacy intrusion generates privacy concerns among individuals and demand policies and regulations by the state. Privacy intrusion is not being constituted negatively by the organizations and government which draw favorable benefits without any loss. Perception of misuse of technology for privacy intrusion is severely felt by the entity suffering individuals. Policymakers should heed attention to the factors which are invisible to logic and reasoning but have an

insidious impact on individuals, groups, and society (Dinev et al., 2015). Privacy protection is affordable for organizations and Governments but individuals, it is a costly affair. So the government has to protect the privacy rights of citizens.

Implications

Privacy study is helpful for sociologists, psychologists, and communications scholars, for individual level of study; scholars of management, information, and organizational behavior studies focus more on the organizational level; and scholars of Law and regulation, and public policy for Government level study. (Ginosar & Ariel, 2017). The study can help to build a strong judicial framework for preparing privacy policy by keeping in view the means of privacy intrusion and its legal enforcement.

Limitation and future scope

An exploratory study was conducted to understand various aspects of privacy intrusion only. This nature of the study limits the periphery. Studies need to be conducted on: privacy intrusion via satellite, electronic gadgets, and advanced technologies. There is a need to focus on government regulations, guidelines, and policies for local and across-boundary privacy intrusion offenses, their remedy, and the development of a strong judicial punishment system for the offender(s)/culprit(s). Reasons for government avoidance of the preparation and enforcement of privacy policy framework require in-depth study. Despite this exploratory research on privacy intrusion, it signifies the prospects for future research in the individual privacy concern domain.

References

Alimatu-Saadia Yussiff, Abdul-Lateef Yussiff, S. J. A. (2013). Internet Privacy: A Survey of Cyber Abuses and Policy Improvements in Ghana. International Journal Information Technology & Electrical Engineering ISSN:, 2(5). https://www.researchgate.net/publication/279196814

Antón, A. I., Earp, J. B., & Young, J. D. (2010). How internet users' privacy concerns have evolved since 2002. In IEEE Security and Privacy (Vol. 8, Issue 1). https://doi.org/10.1109/MSP.2010.38

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. Information and Management, 53(1), 1–21. https://doi.org/10.1016/j.im.2015.08.001

Cheng, C. (2016). The Limits of Privacy. http://about.jstor.org/terms

Clark, T. C., & Westin, A. F. (1968). Privacy and Freedom. California Law Review, 56(3), 911. https://doi.org/10.2307/3479272

Cveticanin, N. (2021). Internet Privacy Statistics to Make You Wonder Who's Got Info on You. https://dataprot.net/statistics/internet-privacy-statistics/

Dinev, T. (2008). Internet users' beliefs about government surveillance - The role of social awareness and internet literacy. In Proceedings of the Annual Hawaii International Conference on System Sciences. https://doi.org/10.1109/HICSS.2008.216

Dinev, T. (2014). Why would we care about privacy? In European Journal of Information Systems (Vol. 23, Issue 2, pp. 97–102). Palgrave Macmillan Ltd. https://doi.org/10.1057/ejis.2014.1

Dinev, T., McConnell, A. R., & Jeff Smith, H. (2015). Informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the "APCO" box. Information Systems Research, 26(4), 639–655. https://doi.org/10.1287/isre.2015.0600

Gandamayu, I. B. M., Antari, N. W. S., & Strisanti, I. A. S. (2022). The level of community compliance in implementing health protocols to prevent the spread of COVID-19. International Journal of Health & Medical Sciences, 5(2), 177-182. https://doi.org/10.21744/ijhms.v5n2.1897

Ginosar, A., & Ariel, Y. (2017). An analytical framework for online privacy research: What is missing? Information and Management, 54(7), 948–957. https://doi.org/10.1016/j.im.2017.02.004

Harsha Vardhini, P. A., & Deepthi, K. (2017). FPGA based brain computer interface system. International Journal of Innovative Research in Science and Engineering, 3(1).

IAPP. (2007). Fair Information Practice Principles. Iapp. https://iapp.org/resources/article/fair-information-practices/

Jeff Smith, H., Dinev, T., & Xu, H. (2011a). Information privacy research: An interdisciplinary review. In MIS Quarterly: Management Information Systems (Vol. 35, Issue 4). https://doi.org/10.2307/41409970

Jeff Smith, H., Dinev, T., & Xu, H. (2011b). Information privacy research: An interdisciplinary review. In MIS Quarterly: Management Information Systems (Vol. 35, Issue 4, pp. 989–1015). University of Minnesota. https://doi.org/10.2307/41409970

Jos, P. H. (2006). Social contract theory: Implications for professional ethics. American Review of Public Administration, 36(2), 139–155. https://doi.org/10.1177/0275074005282860

Jovanovic, B. (2022). Better safe than sorry: Cyber security statistics and trends for 2021. DataProt. https://dataprot.net/statistics/cyber-security-statistics/

King, S. T., & Chen, P. M. (2003). Backtracking intrusions. In Operating Systems Review (ACM) (Vol. 37, Issue 5). https://doi.org/10.1145/1165389.945467

Kumaraguru, P., & Cranor, L. F. (2005). Privacy Indexes: A Survey of Westin's Studies. http://www.pandab.org/RptOrderForm.pdf

Park, J. S., & Sandhu, R. (2000). Secure cookies on the web. IEEE Internet Computing, 4(4), 36–44. https://doi.org/10.1109/4236.865085

Pedersen, D. M. (1997). Psychological functions of privacy. Journal of Environmental Psychology, 17(2), 147–156. https://doi.org/10.1006/jevp.1997.0049

Purplesec. (2021). 2021 cyber security statistics: The ultimate list of stats, data & trends. Purplesec. https://purplesec.us/resources/cyber-security-statistics/

Regan, P. M. (2002). Privacy as a Common Good in the Digital World. Information, Communication & Society, 5(3), 382–405. https://doi.org/10.1080/13691180210159328

Sipior, J. C., Ward, B. T., & Rongione, N. M. (2004). Ethics of collecting and using consumer internet data. Information Systems Management, 21(1), 58–66. https://doi.org/10.1201/1078/43877.21.1.20041201/78986.6

Smith, K. T. (2011). Digital marketing strategies that Millennials find appealing, motivating, or just annoying. Journal of Strategic Marketing, 19(6), 489–499. https://doi.org/10.1080/0965254X.2011.581383

Sobers, R. (2021). 134 Cybersecurity Statistics and Trends for 2021. Inside Out Security Blog, Data Security. https://www.varonis.com/blog/cybersecurity-statistics

Spajic, D. J. (2021). Piracy is back: Piracy Statistics for 2021. Dataprot. https://dataprot.net/statistics/piracy-statistics/

Spake, D. F., Zachary Finney, R., & Joseph, M. (2011). Experience, comfort, and privacy concerns: Antecedents of online spending. Journal of Research in Interactive Marketing, 5(1), 5–28. https://doi.org/10.1108/17505931111121507

Suryasa, I. W., Rodríguez-Gámez, M., & Koldoris, T. (2021). Get vaccinated when it is your turn and follow the local guidelines. International Journal of Health Sciences, 5(3), x-xv. https://doi.org/10.53730/ijhs.v5n3.2938

TitanFile. (2022). 7 Data Privacy Statistics that May Surprise You! https://www.titanfile.com/blog/7-data-privacy-statistics-that-may-surprise-you/

Van Aaken, D., Ostermaier, A., & Picot, A. (2014). Privacy and freedom: An economic (Re-)evaluation of privacy. Kyklos, 67(2), 133–155. https://doi.org/10.1111/kykl.12047

Warren, S. D., & Brandeis, L. D. (2005). The right to privacy. Information Ethics: Privacy, Property, and Power, 209–225. https://doi.org/10.7312/gold91730-002

Weber, R. H. (2015). The digital future - A challenge for privacy? Computer Law and Security Review, 31(2), 234–242. https://doi.org/10.1016/j.clsr.2015.01.003

Westin, A. F. (1968). Privacy And Freedom. Washington and Lee Law Review, 25, 3–4. https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20

Wilkins, A. (2021). Water on Mars: Large deposits found below the surface at the equator | New Scientist. https://www.newscientist.com/article/2302207-large-deposits-of-water-found-on-mars-below-the-surface-at-the-equator/

Xu, H., Teo, H. H., Tan, B. C. Y., & Agarwal, R. (2012). Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. Information Systems Research, 23(4), 1342–1363. https://doi.org/10.1287/isre.1120.0416

Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. In Journal of Network and Computer Applications (Vol. 84, pp. 25–37). Academic Press. https://doi.org/10.1016/j.jnca.2017.02.009