Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 5 Issue 4 (2025)

Security and Privacy Issues Related to Electronic Documents based on the Public Perception

Dr. Farhana Islam

Lecturer, Farmingdale State College,

State university of New York

Abstract

This paper aims to investigate the security issues and risks to privacy associated with electronic documents (e-documents) within an organization. This paper also emphasis on new technologies applied to documents and document handling. Electronic Document encourages significant improvements in productivity and performance. A Document Management System (DMS) typically refers to the use of a computer system and software to store, organize, and manage electronic records and scanned versions of paper documents. This paper explains the ways in which the security and privacy of users are maintained when they access electronic documents through sharing or use. According to the public perception the dimensions of the security and privacy measurement are selected. This paper through answering the research questions, describes the measures that companies are maintaining privacy and security to preserve e-business document confidentiality. It also discusses the public perception of e-document privacy and security. In the conclusion, further recommendations specify how the firms should make a balance between the privacy and security issues in their e-documents.

Keywords: Information Management, Access Control, Organizational Technology, Data Protection, Business Systems, Content Analysis

Introduction

Muftic, bin Abdullah & Kounelis (2016) point out that the leading value of electronic document (e-document) management today lies in the ability to quickly access data and information. There are just two fundamental approaches to consider when thinking about data access. The first action is to set up electronic documents properly which needs a bit of discipline initially. Those who are skilled at filing usually use neat file systems. Programs on computers help to alphabetize, organize, and store data securely and maintain it properly. In the second paradigm, unstructured data is the key method for obtaining documents.

According to Pleger, Guirguis & Mertes (2021), being overloaded with work means people are overwhelmed by data and are unlikely to organize it the way it should be. Digital solutions can be found for every problem. At present, in the office e-mail, e-fax, and instant messages have taken the place of paper documents. When the technology emerged in the offices the issues of their privacy and security were raised. Documents security involves keeping all forms of data safe from being accessed, used, examined, disclosed, modified, copied, moved or destroyed by anyone without permission. Document privacy or data privacy, connects the way data is handled with the public's belief in privacy. Keshta & Odeh (2021) focused his article on social theory to look at how security is involved with human roles, actions, goals and policies. Fabrègue & Bogoni (2023) demonstrates the significant role of information security in operating a business. Risk analysis was done with organizational analysis using agents, activities, resources, information, assets and roles as a basic structure. Cherif & Mzoughi (2022) pointed out that organizing how to use and secure Information Systems (IS) is necessary. This research paper describes the public perception of security, privacy and digital technology towards the e-documents.

Research Questions:

- What are the measures that companies are maintaining privacy and security to preserve e-business document confidentiality?
- What is the public perception of e-document privacy and security?

Literature Review

Concepts of E-Documents in Business

According to a study by records managers, there are 318 billion pieces of paper stored and every year 92 billion more pages are added. Every year, computers produce about 775 billion printed pages. It was estimated that in 1990, 3.1 million tons of paper were needed for these new documents. Saeed (2023) reported that the bulk of paperwork is made up of business documents. A research firm reports that American companies annually spend over $6 billion on preprinted forms and throw out more than $2 billion.

Kojima & Iwata (2012) write that document imaging turns paper into electronic form to increase company efficiency and guarantee proper handling of those documents. They also explained in their articles that one document could go through the hands of five or six people or be processed that many times by the same person in a paper-based setting. In a regular office setting, tasks such as receiving a shipment, filling the order, paying the invoice, issuing and sending out a check and then mailing both the check and a copy to the seller need to be done by handling the invoice (Suhartono, Setiawan & Irwanto, 2014). It was argued that paper exists only at a single location, access is not always available, the chance of losing it by accident or catastrophe is significant and the expense of routinely working with it is considerable.

As technological changes in managing these documents occurred rapidly, a document management system started to become necessary. The authors introduced *"The One Base software"* which enables someone to search within the full text of images that have been scanned. Camenisch, Lehmann & Neven (2012) wrote about the possibility of a medical office without paperwork. According to the researchers, a digital hospital system that has patient records, and voice recognition systems and uses email correspondence for communication can enhance patient care, save costs and improve efficiency. Sivan & Zukarnain (2021) found from 1989 to 1997, the proportion of office workers using computers in Sweden went up from 65% to 90%. The percentage of women with jobs also rose, to 94%, in 1999. During these years, organizations found ways to convert paper records into digital form by using new methods of handling documents.

The goal was to provide information to a wider range of users whenever and wherever they required it and to improve the speed, quality and effectiveness of handling documents. Based on data from Imersion Technologies, Inc.:

- Around 90% of a company's memory is stored on paper.
- Most days, 90% of the pages used in an office just go back and forth and remain unchanged.
- It is common for a document to be copied 19 times.
- Documentation services would charge $20 for filing a file, $120 for searching for a file that was misplaced and $220 to re-create a missing document.
- About 7.5% of all documents are lost and another 3% end up being misfiled.
- It takes professionals between 5-15% of their time to read information, and as much as 50% to find it.
- Some experts estimate over 4 trillion paper documents in the U.S., with a 22% rise every year.

Articles written by different authors mostly agree on how the electronic document system is changing the working patterns inside a business organization. They suggest different software and technology for document management systems. As a result, ensuring e-document safety and privacy is gaining importance. Document management using Information Technology (IT) is a key challenge for IS managers (Suhartono, Setiawan & Irwanto, 2014). Much of what matters in organizations is kept as written material such as business forms, reports, letters, memos, policy statements, contracts and agreements. At the same time, business flows are often influenced by the activity of paperwork. An electronic document is defined as:

- ***Electronic:*** Making use of today's information and communication technologies.
- ***Document***: Details about a subject, arranged for people to understand, are represented by symbols and are stored and managed as one single unit.

Concepts of Security

Lee, Hess & Heldeweg (2022) describes security as feeling assured that there is equilibrium between risks and controls on information. Lin, Carter & Liu (2021) pointed out that information security protects information and reduces the chance of others seeing it. Computer fraud and abuse may have already caused significant losses and the risk is still very high. Due to new technological developments, the white hats now have many methods for combating these threats. The technological advances have equipped the white hats with numerous effective countermeasures.

According to Wen et al. (2023), in his article, he identifies several security measures based on appropriate technology. In his article, he mentioned four security measurement information technologies, and among those, the most important are in any business organization: (1) physical countermeasures and (2) computer-technology countermeasures.

According to Reegu et al. (2023), physical countermeasure includes the electronic surveillance of people and objects. This new surveillance technology differs from traditional social control in that (1) the technology is not impeded by distance, darkness, or physical barriers; (2) records are provided for easy storage, retrieval, and analysis; (3) the concern is with reducing risk and un- certainty; and (4) those under surveillance often become active partners in their monitoring.

According to Zhang, Xue & Liu (2021), locks, passwords, access codes, and access cards are also physical countermeasures. Small cards may use different technologies, including magnetic stripe, magnetic dot, embedded wire, or passive proximity. He suggested in his article that each technology has its advantages and disadvantages and should be selected based on an informed definition of what the access-control system is intended to accomplish. He discussed that the effectiveness of the cards depends on the protection they receive from holders and on how difficult they are to forge or alter.

Computer technology encounters include some technology that allows the machine to perform several unsuccessful access attempts and machine searches of a table of authorized transactions or authorized users, as well as the extent of their authority. Houser, Flite & Foster (2023) explains encryption and data automation, which serve as security measures in computers, as described in his article.

Concepts Privacy

According to Hwang and Lai (2015), privacy is a significant issue connected to documents. Any proven fair protocol for document exchange must incorporate privacy. When dealing with paperwork in a company, a notary only notarizes each document just once. The owner of an authorized document can share it with multiple parties and multiple times, ensuring that only the intended participants can access the document's source.

In their published paper, they introduced a new protocol. Their suggested protocol verifies a document only once and issues the recovery certificate to the responsible person. Under the proposed protocol, documents that can be verified do not have to be notarized. When the authorized party has notarized their document, they can use the recovery certificate to transfer it to others without compromising transaction privacy. After notarizing, the online notary is no longer required to retain or record any messages or maintain a public catalog. Therefore, the protocol is practical and saves costs in multi-receiver e-business scenarios.

Blaauw (2013) gave his definition of privacy in his work. He described privacy as not sharing certain private propositions with others; a lack of privacy means that these private propositions are known to others. They introduced the idea of three argument places called a subject (S), a set of propositions (P), and a set of individuals (I). The subject or the person concerned is what is represented by "S" and their privacy. Those propositions the author wants to keep private are in "P," and those individuals aiming to conceal these propositions are in "I."

Paul et al. (2023) referred to informational privacy as 'data protection.' He believes that data protection is the best example of matching privacy matters with the influence of technology since it's easier to see what is meant by data protection and how technology can help protect it. According to Van den Hoven, Lokhorst & Van de Poel (2021), this leads users to further ask why privacy matters and why the data should be protected.

Concept of Public Perception

Public perception, according to Wolfgang Donsbach (2008), is made up of what the majority of people in a country want or believe about a matter or problem. According to (Clarke, 2009), 'the public' is discussed as a special kind of group

behavior consisting of those individuals currently talking or thinking about a particular subject. Danezis, Diaz, and Troncoso (2007) noted that media and public relations have a significant impact on public opinion and perception. In his view, people's opinions are shaped by their current circumstances, social backgrounds, and the knowledge and beliefs they hold. Discussing well-known issues can significantly impact the way the public perceives opinion leaders.

Methods

Content analysis has been chosen for this research question because it is an established research tool in the field of Journalism and Mass Communication. The goal of this paper is to analyze and summarize the main ideas and arguments put forward in recent works. According to Lin, J., Carter & Liu (2021), content analysis is valuable for study in Library Science as it examines the characteristics within recorded data. Wu, Dwivedi, & Srivastava (2021) noted that content analysis refers to an organized approach to studying the elements of communication.

Messages in content analysis can reveal both the open and subtle concepts present in the material. Manifest content appears clearly within the message itself. An illustration is that a specific word itself appearing in a text is manifest content. The decision to display a photograph in color or black & white on a website reveals the manifest content. Since latent content is a concept, it does not appear clearly in the messages. According to Pleger, Guirguis & Mertes, (2021), content analysis is limited to studying manifest content. Nevertheless, most content analysis researchers argue that latent content features can be analyzed by looking at manifest indicators.

Content Analysis is used to identify key organizational factors that play a significant role in securing e-documents. The key factors for securing Electronic Document Management Systems are identified as essential functions for each company to maintain privacy and security. A coding schema inherits these functions to analyze the e-document confidentiality and security (Bandura & Donsbach, 2008). Each coding entry is supported by the corresponding public perception statistical data, providing a clear understanding of the confidentiality of each security function.

Coding Schema for E-document Security and Privacy

Table 1: Key Implementation Controls for Electronic Document Management System

Corresponding Security Measure	Definition
Consent	Ensure users consent to having their data collected and used for other purposes, if necessary.
Notice	Allow users to be alerted when their data will be used differently or shared with third parties.
Access	Only allow accredited individuals and companies to gain access.
Use	Reduce the use of company assets to what is really needed to support business goals.
Retention	Keep information only if it is needed for proper business use.
Security	Ensure information is securely protected.
Audit Trail	Save a history or record of all activities related to information.
Review	Allow individuals to access their files to look at and edit their personal details.

(Source: Madden, 2014)

Findings

Table 2: Key Implementation Controls for Electronic Document Management System and Public Perception Level

Corresponding Security Measure	Public Perception Level
Consent	• 54% net of Americans sharing information and consent is difficult.
Notice	• 52% of Americans said they are either very worried or somewhat worried about

	security and privacy agreements. • About 89% of consumers said they felt more comfortable sharing information with a company that displayed a well-written privacy policy.
Access	• Up to 70% of social networking site users are at least somewhat concerned that their information could be accessed by the government without them knowing.
Use	• Almost all adults (93%) believe that having a say over who accesses their information is crucial; 74% call it very important and 19% consider it somewhat important.
Retention	• About 55% of people living in the United States have an online account for banking or financial services. • Around 36% of people are registered with household utility companies online. • More than a quarter (32%) of Americans use online accounts to access their healthcare records. • 39% own online accounts that are used for handling payments or transactions. • About 28 per cent of Americans say they have low confidence in the federal government protecting their information, while only 12 per cent say they are very confident. • Almost three times as many social media users do not trust sites to keep their details safe (24%) as there are people who do (9%). • Around 40% say that information about their online actions should not be saved by their search engine. • Around half of adults feel that ads placed by online advertisers shouldn't remain in their browser data for much time. • 44% believe that the history of their video viewing on online sites should not be stored.
Security	• Up to 24% of those who use the internet keep a list of their passwords in a digital document on their devices and 18% use the auto-save function most browsers offer • Around 52% of people with internet access have used two-factor authentication on their accounts. • 40% of people who have suffered a breach of their social media accounts are not at all convinced that the platforms can keep their personal details safe.
Audit Trail	• • A small group of adults, just 6%, believe government agencies can fully keep their records secure and private, while another 25% are somewhat confident • The results show that 6% are very certain and 25% are somewhat certain landline companies will protect their data. • Credit card companies seem to give people a higher degree of confidence; 9% feel very secure and 29% feel reasonably secure with their information. • 50% of adults think that online advertisers who place ads on the websites they visit should not save records or archives of their activity for any length of time.
Review	• More than 40% think that social media sites should not gather data regarding how they use the service. • About 39% of those with difficulty managing passwords also mention another similar concern.

(Source: Madden & Raine, 2015)

The public believes that there should be stronger social systems in place to protect electronic document privacy and security where the public views each coding system as a vital means to control the privacy and security of documents. Access control enables individuals to determine who or what has access to various resources within a computing

environment (Olmstead & Smith, 2017). Based on Andrew Johnson's research (2016), there are mainly two ways to control and manage e-documents: physical and logical. Access control is set up to control who is able to enter campuses, buildings, rooms, and IT assets within the organization.

It supplies rules that prevent unauthorized people from accessing computer networks, system resources, and information. According to Lin, Feng, and Li (2017), in their article, access control is an effective way to secure user information and prevent leaks from occurring. Having access control ensures users are granted permission to access the network and stops illegal interference or accidental damage caused by users who mistakenly operate the network. The use of passwords, PINs, smart cards, and biometric measures in organizations assures privacy and security in documents.

The security of electronic documents is also a crucial consideration. Madden & Raine (2015) stated that having strong passwords, clearing out drives, creating secure message protocols (SMPs), utilizing alarms and cameras, and choosing floor marshals are effective measures for security on e-documents. Keshta & Odeh (2021) highlight that the proper security of documents relies on the privacy of communications, secure storage of data, user authentication, fine-tuned access rights, confidentiality, and integrity.

A document retention and destruction policy outline the procedures for staff, volunteers, board members, and external parties to manage and maintain the organization's documents. Any organization should have clear guidelines about which documents must be stored in the Cloud, on a server, or in a file cabinet. Topics relating to the handling of documents are central to over half the comments in Pew Research's survey (Olmstead & Smith, 2017). Using mail, text messaging, apps, social sites, Cloud storage, and voice mail allows organizations to record vital information. Organizations are responsible for creating policies that determine how long and how to store their documents securely. Companies should build their policies around e-documents, considering how records are assembled and maintained. A retention policy can refer to the following items:

- Figure out who will manage the DRP.
- Find out which documents, whether physical or electronic, the company makes use of.
- Make a decision regarding how long documents should be stored.
- Pick a location and a system for storing the documents.
- Decide on the ways that documents should be destroyed.
- Keep the files and records according to the standards in the retention policy.

88% of Internet users would prefer that companies ask for approval before giving away their personal information online (Cherif & Mzoughi, 2022). 56% of Americans are more likely to refuse any personal data collection, and another 34% would opt out sometimes. Fabrègue & Bogoni (2023) have established a process for providing information before consenting to treatment. He believes that disclosure, comprehension, voluntariness, competence, agreement, and minimal distraction should be the main elements of providing information consent. The six components listed here should be used to check the basic consent of e-documents.

All organizations should communicate clearly with their staff, employees, and stakeholders by using written notices to make better use of electronic documents. Employees would learn and understand their access rights and what they are expected to do with the e-documents as outlined in the notice. An auditing process may count on both classic logging systems and existing modern auditing mechanisms. According to Saeed (2023), auditing is explained and linked to the document management system in his book. He focused on what auditors should pay attention to keep documents secure and private.

- **Data Centre Personnel**: Data center staff should have appropriate access to the facility with IDs, login IDs and secure passwords.
- **Equipment**: The proper functioning of all equipment found in the Data Center should be checked by the auditor.
- **Policies and Procedures**: Written documentation and procedures for the Data Center should be located in the center for referral and application.

- **Physical Security / Environmental Controls:** The auditor should examine the client's security for the Data Center. Security of physical spaces includes bodyguards, locked cages, man traps, singular entrances, equipment that is fastened to the ground and monitoring systems for computers.
- **Backup Procedures**: The auditor should confirm that the client can recover data if their system fails by looking at their backup measures. Clients might choose to have a second Data Center located elsewhere, so they can use it instantly in case the main system is not working.

It is necessary to manage access to electronic documents. The distribution of information and its channels plays a significant role. System software is used to monitor how documents are being used (Council of Nonprofits.org, 2025). Those who control the e-documents use programs such as *e-file Cabinet, Content Central, View Centre, Canvas, File Hold, and Intranet Dashboard.* Each electronic document can be categorized under different categories while it is being reviewed. Documents that do not need to be deleted anymore to clear up the hard drive's space.

If numerous documents need electronic review, the organization may resort to Indexing data and documents. According to Sivan & Zukarnain (2021), indexing data and documents is essential in electronic documents. Index data can contain information about individuals, making it a crucial point for privacy protection measures. Second, because it describes the content of documents, metadata can be included in privacy protection measures.

Conclusions

Electronic documents have to follow the same rules as any other type of information system. At the same time, following these rules depends on analyzing documents. This research paper concludes that the public agrees that e-documents should be managed with the eight specified security and privacy measures. While security measures can be challenging, they can still be managed effectively. It is essential to consider and manage several risks when implementing security tools for e-documents during the system's design phase. Organizations need to clearly define the privacy and security standards for their electronic document management systems, identify the privacy risks associated with electronic documents, and train their staff to apply appropriate privacy precautions when working with electronic records.

Implications

The research reveals significant gaps between what the public expects in terms of electronic document security and privacy and the current practices in organizations. The substantial gap between people's expectations for data security and the policies they believe companies are implementing impacts business processes, adherence to the law, and consumers' trust. Companies should note that the majority of customers think that information handling and consent shouldn't be a concern, and about half still feel uncomfortable about sharing their information. It suggests that today's privacy rules and security protocols fail to address people's concerns adequately.

According to the study, focused security is not only a technological requirement but also necessary to sustain customer confidence and competitiveness. Firms failing to handle all these aspects, including consent, notice, access, use, retention, security, audit trail, and review, may lose customer trust and be subject to fines from regulators. Poor public confidence in ensuring privacy suggests that organizations need to actively manage this issue.

Additionally, the research suggests that the public is most concerned about transparency and the ability to control their data. Because a substantial number of individuals are concerned about managing their access and worry about the government viewing their records, organizations should enhance their access controls and establish clearer communication channels. Firms should shift their practices from only complying with the law to securing user control and honesty when handling their documents. This means that rules and regulations can be updated to address better the gap between the public's expectations and the current state of electronically managing records.

Further Research

In the future, researchers should assess whether particular privacy-enhancing technologies can address people's concerns when it comes to safeguarding electronic documents. Such studies would demonstrate how people perceive an organization once its security practices are enhanced, providing valuable insights into public trust and effective company

management. Furthermore, studying the ways privacy and security are managed globally can help businesses develop effective document management strategies that are applicable everywhere. Examining the economic implications of stricter privacy rules versus the consequences of security breaches would help organizations make more informed investment decisions.

References

1. Bandura, A., & Donsbach, W. (2008). International encyclopedia of communication. *Blackwell google schola CBSE/Artificial intelligence curriculum google schola Chamizo, JA/2013/A new definition of models and modeling in chemistry's teaching/Science & Education*, *22*(7), 1613-1632. https://bibbase.org/network/publication/bandura-donsbach-internationalencyclopediaofcommunication-2008
2. Blaauw, M. (2013). The epistemic account of privacy. *Episteme*, *10*(2), 167-177. https://philpapers.org/archive/BLATEA.pdf
3. Camenisch, J., Lehmann, A., & Neven, G. (2012). Electronic identities need private credentials. *IEEE Security & Privacy*, *10*(1), 80-83. https://www.profsandhu.com/cs6393_s13/2.%20camenisch_etal_2012.pdf
4. Cherif, E., & Mzoughi, M. (2022). Electronic health record adopters: a typology based on patients' privacy concerns and perceived benefits. *Public Health*, *207*, 46-53. https://uca.hal.science/hal-03806662/file/S0033350622000853.pdf
5. Clarke, R. (2009). Privacy impact assessment: Its origins and development. *Computer law & security review*, *25*(2), 123-135. http://www.rogerclarke.com/DV/PIAHist-08.html
6. Councilofnonprofits.org, (2025). *Document Retention Policies for Nonprofits.* https://www.councilofnonprofits.org/tools-resources/document-retention-policies-nonprofits
7. Danezis, G., Diaz, C., & Troncoso, C. (2007). Two-sided statistical disclosure attack. In *Privacy Enhancing Technologies: 7th International Symposium, PET 2007 Ottawa, Canada, June 20-22, 2007 Revised Selected Papers 7* (pp. 30-44). Springer Berlin Heidelberg. https://lirias.kuleuven.be/retrieve/333423
8. Deacon, D. (2007). Yesterday's papers and today's technology: Digital newspaper archives and 'push button'content analysis. *European journal of communication*, *22*(1), 5-25. https://repository.lboro.ac.uk/articles/journal_contribution/Yesterday_s_papers_and_today_s_technology_digital_newspaper_archives_and_push_button_content_analysis/9475490/1/files/17100002.pdf
9. Fabrègue, B. F., & Bogoni, A. (2023). Privacy and security concerns in the smart city. *Smart Cities*, *6*(1), 586-613. https://www.mdpi.com/2624-6511/6/1/27/pdf
10. Houser, S. H., Flite, C. A., & Foster, S. L. (2023). Privacy and security risk factors related to telehealth services–a systematic review. *Perspectives in health information management*, *20*(1), 1f. https://pmc.ncbi.nlm.nih.gov/articles/PMC9860467/pdf/phim0020-0001f.pdf
11. Hwang, R. J., & Lai, C. H. (2015). Provable fair document exchange protocol with transaction privacy for e-commerce. *Symmetry*, *7*(2), 464-487. https://www.mdpi.com/2073-8994/7/2/464
12. Jackson, M. (2008). Content analysis. *Research methods for health and social care*, 78-91. https://books.google.com/books?hl=en&lr=&id=IiFHEAAAQBAJ&oi=fnd&pg=PA78&dq=Berelson,+B.+(1954)+Content+Analysis.&ots=PUPz0TN3hY&sig=SYg_k92xi8b_Y6TAfmx0WlK6vmU
13. Josang, A., AlZomai, M., & Suriadi, S. (2007). Usability and privacy in identity management architectures. In *ACSW Frontiers 2007: Proceedings of 5th Australasian symposium on grid computing and e-research, 5th australasian information security workshop (privacy enhancing technologies), and Australasian workshop on health knowledge management and discovery* (pp. 143-152). Australian Computer Society. https://eprints.qut.edu.au/7289/1/JAS2007-AISW.p**df**
14. Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal*, *22*(2), 177-183. https://www.sciencedirect.com/science/article/pii/S1110866520301365
15. Kojima, H., & Iwata, K. (2012). Seamless management of paper and electronic documents for task knowledge sharing. *Electronics and Communications in Japan*, *95*(8), 52-63. https://onlinelibrary.wiley.com/doi/abs/10.1002/ecj.10370

16. Lee, D., Hess, D. J., & Heldeweg, M. A. (2022). Safety and privacy regulations for unmanned aerial vehicles: A multiple comparative analysis. *Technology in Society*, *71*, 102079. https://www.sciencedirect.com/science/article/am/pii/S0160791X22002202
17. Lin, C., Feng, F. J., & Li, J. S. (2017). Access control in new network environment. *Ruan Jian Xue Bao(Journal of Software)*, *18*(4), 955-966. https://scispace.com/pdf/access-control-in-new-network-environment-15w3ur1cwo.pdf
18. Lin, J., Carter, L., & Liu, D. (2021). Privacy concerns and digital government: exploring citizen willingness to adopt the COVIDSafe app. *European Journal of Information Systems*, *30*(4), 389-402. https://www.researchgate.net/profile/Jiesen-Lin/publication/351353312_Privacy_concerns_and_digital_government_exploring_citizen_willingness_to_adopt_the_COVIDSafe_app/links/66271b9c39e7641c0be2f0bd/Privacy-concerns-and-digital-government-exploring-citizen-willingness-to-adopt-the-COVIDSafe-app.pdf
19. Madden, M. & Raine, L. (2015). *Americans' Attitudes About Privacy, Security and Surveillance.* http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/
20. Madden, M. (2014). *Public Perceptions of Privacy and Security in the Post-Snowden Era.*
21. Muftic, S., bin Abdullah, N., & Kounelis, I. (2016). Business information exchange system with security, privacy, and anonymity. *Journal of Electrical and Computer Engineering*, *2016*(1), 7093642. https://onlinelibrary.wiley.com/doi/pdf/10.1155/2016/7093642
22. Neuendorf, K. A. (2017). *The content analysis guidebook*. sage. https://howardaudio.wordpress.com/wp-content/uploads/2018/01/content-analysis-in-the-interactive-media-age.pdf
23. Olmstead, K & Smith A. (2017). *2. Password management and mobile security.* http://www.pewinternet.org/2017/01/26/2-password-management-and-mobile-security/
24. Paul, M., Maglaras, L., Ferrag, M. A., & Almomani, I. (2023). Digitization of healthcare sector: A study on privacy and security concerns. *ICT express*, *9*(4), 571-588. https://www.sciencedirect.com/science/article/pii/S2405959523000243
25. Pleger, L. E., Guirguis, K., & Mertes, A. (2021). Making public concerns tangible: An empirical study of German and UK citizens' perception of data protection and data security. *Computers in Human Behavior*, *122*, 106830. https://www.sciencedirect.com/science/article/pii/S0747563221001539
26. Reegu, F. A., Abas, H., Gulzar, Y., Xin, Q., Alwan, A. A., Jabbari, A., ... & Dziyauddin, R. A. (2023). Blockchain-based framework for interoperable electronic health records for an improved healthcare system. *Sustainability*, *15*(8), 6337. https://www.mdpi.com/2071-1050/15/8/6337/pdf
27. Rubel, A. (2011). The particularized judgment account of privacy. *Res Publica*, *17*, 275-290. https://philarchive.org/archive/RUBTPJ
28. Saeed, S. (2023). A customer-centric view of E-commerce security and privacy. *Applied Sciences*, *13*(2), 1020. https://www.mdpi.com/2076-3417/13/2/1020/pdf
29. Sivan, R., & Zukarnain, Z. A. (2021). Security and privacy in cloud-based e-health system. *Symmetry*, *13*(5), 742. https://www.mdpi.com/2073-8994/13/5/742/pdf
30. Suhartono, D., Setiawan, E., & Irwanto, D. (2014). Electronic Document Management Using Inverted Files System. In *EPJ Web of Conferences* (Vol. 68, p. 00004). EDP Sciences. https://www.epj-conferences.org/articles/epjconf/pdf/2014/05/epjconf_icas2013_00004.pdf
31. Van den Hoven, J., Lokhorst, G. J., & Van de Poel, I. (2012). Engineering and the problem of moral overload. *Science and engineering ethics*, *18*, 143-155. https://link.springer.com/content/pdf/10.1007/s11948-011-9277-z.pdf
32. Wen, B., Wang, Y., Ding, Y., Zheng, H., Qin, B., & Yang, C. (2023). Security and privacy protection technologies in securing blockchain applications. *Information Sciences*, *645*, 119322. https://www.sciencedirect.com/science/article/pii/S0020025523009076
33. Wu, H., Dwivedi, A. D., & Srivastava, G. (2021). Security and privacy of patient information in medical systems based on blockchain technology. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, *17*(2s), 1-17. https://orbit.dtu.dk/files/262411019/Article22_Shuai.pdf
34. Zhang, R., Xue, R., & Liu, L. (2021). Security and privacy for healthcare blockchains. *IEEE Transactions on Services Computing*, *15*(6), 3668-3686. https://arxiv.org/pdf/2106.06136