Security and Privacy Concerns in Information Usability

Liang-Chih Yang
Center for General Education / Graduate School of Criminology
National Taipei University
New Taipei City , Taiwan
kevin@gm.ntpu.edu.tw

Abstract

This paper explores the current state of security and privacy in information usability. It examines the current legal and technological frameworks surrounding the issue, as well as the impact of these frameworks on businesses and individuals. Additionally, the paper looks at potential solutions for improving security and privacy in information usability, including improved data management policies and the use of encryption. Finally, the paper considers the implications of the current state of security and privacy on the future of information usability.

1. Introduction

Information usability has become increasingly important in today's digital era. As more and more data is collected and shared, the need for secure and private information usability has become paramount. This paper will explore the current state of security and privacy in information usability, including the legal and technological frameworks surrounding it, and its implications for businesses and individuals. Furthermore, the paper will suggest potential solutions for improving security and privacy in this area and examine the implications of the current state of security and privacy on the future of information usability.

1.1 Information usability

Information usability is the ability of information to be understood and utilized by people in order to achieve a desired outcome. It encompasses the usability of digital content such as websites, documents, mobile applications, interactive media, and other information-based products. Information usability focuses on the user experience, taking into account factors such as ease of use, accessibility, and the relevance of the content. It also considers the user's knowledge and skills, as well as the context in which the information is used. Good usability helps users quickly and accurately find and understand the information they need, without getting frustrated or overwhelmed. Poor usability can lead to confusion and frustration, resulting in users abandoning their task and potentially not returning. Information usability is therefore important for creating a positive user experience and ensuring that users are able to find the information they need.

1.2 Current issues about information usability

Information usability is a crucial aspect of designing effective systems and interfaces. However, there are still several unanswered questions in this field that require further research and investigation. One major unanswered question is the challenge of extracting usable information from unstructured big data (Adnan et al., 2021). Unstructured big data poses challenges due to its diversity, sparsity, and heterogeneity issues. Developing

a usability enhancement model for unstructured big data would greatly contribute to improving the usability of information extracted from such data.

Another unanswered question relates to the usability of mobile applications (Harrison et al., 2013). While there are existing usability models, they often overlook important attributes such as cognitive load, which can significantly impact the success or failure of an application. Therefore, there is a need for a new usability model that takes into account these overlooked attributes to ensure the usability of mobile applications.

In the context of healthcare, there are unanswered questions regarding the usability of information systems integrated into hospital settings (Nabovati et al., 2014). Usability evaluation of laboratory and radiology information systems integrated into a hospital information system revealed major usability problems, particularly in the area of "help and documentation." Addressing these usability issues is crucial to ensure efficient and effective use of information systems in healthcare settings.

Additionally, there are unanswered questions about the usability of information in the field of community pharmacy (Gordon et al., 2011). The nature of these unanswered questions mainly revolves around potential or perceived medication-related adverse effects and the need for information to guide the selection of medicines or treatment. Addressing these questions would greatly contribute to improving the usability of information in community pharmacy settings.

In conclusion, there are several major unanswered questions about information usability. These include challenges related to extracting usable information from unstructured big data, improving the usability of mobile applications, addressing usability issues in healthcare information systems, and providing relevant information in community pharmacy settings. Further research and investigation in these areas are necessary to enhance the usability of information and improve user experiences.

2. Legal and Technological Frameworks

2.1 GDPR and CCPA

The legal and technological frameworks surrounding security and privacy in information usability are complex and constantly evolving. As of now, there are various laws and regulations that govern the use of data, such as the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). These laws provide users with certain rights regarding their data, such as the right to access, delete, and rectify the data. Additionally, there are a number of technological solutions that have been developed to help protect data, such as encryption and data masking. These solutions can be used to protect data from unauthorized access and ensure its privacy.

2.2 The increased prevalence of technology

The increased prevalence of technology and its associated data has resulted in a heightened focus on security and privacy in information usability, as users must be assured that their data is secure and protected from unauthorized access. This thesis focuses on the importance of security and privacy considerations in information usability, examining how the combination of technology, security and privacy can be used to create a secure and efficient user experience. It will also explore the potential risks and benefits of using technology to improve information usability, as well as how security and privacy can be effectively implemented in this context. Ultimately, this thesis will provide an in-depth overview of the role of security and privacy in information usability, providing a better understanding of the key challenges and benefits that need to be addressed when deploying technology in this setting.

Security and privacy are essential aspects of information usability. With the rise of technology and the internet, it has become increasingly important to ensure

that users' data is secure and private.

3. Impact on businesses and individuals

Security and privacy are essential to the proper functioning of information usability. Without proper protection, businesses and individuals could be exposed to potential risks, such as data breaches, identity theft, and malicious attacks. For businesses, these risks can lead to costly fines and reputational damage, as well as a loss of customer trust. For individuals, the risks could lead to a loss of privacy and the potential for identity theft. As such, it is essential that businesses and individuals take steps to ensure their data is secure and private.

Security and privacy concerns are significant when it comes to information usability. The literature confirms that the ease of navigation and perceived usefulness of available information directly impact the adoption and sustained use of technology (Irizarry et al., 2015). In the context of mobile health systems, which often deal with sensitive patient information, there are several privacy and usability issues that need to be addressed (Katusiime & Pinkwart, 2017). Usability principles, such as coherent presentation of information and providing up-to-date and accurate information, are crucial for the effective design of electronic medical records interfaces (Zahabi et al., 2015).

When deploying information and communication technology solutions for informal caregivers, challenges related to technology design and usability, as well as concerns about privacy and data autonomy, need to be considered (Hassan, 2020). Similarly, when developing technology to assist aging in place, concerns about usability, information security, and privacy must be addressed to ensure user acceptance (Elers et al., 2018). The poor usability of privacy controls can be seen as an information security vulnerability, highlighting the importance of considering usability in privacy protection (Yankson et al., 2021).

Security, privacy, and usability are among the most important concerns in system and application design (Justine et al., 2018). It is essential to incorporate the human facet of security and consider usability concerns when developing systems and services (Naqvi et al., 2020). Designers should prioritize usability concerns alongside security to ensure that user authentication interfaces in mobile devices are effective and user-friendly (Liang et al., 2014). Usability attributes play a crucial role in software risk evaluation and prioritization, emphasizing the importance of considering usability in the context of achieving specified goals (Jnr, 2019).

In summary, security and privacy concerns are closely intertwined with information usability. Addressing usability issues, such as ease of navigation and effective information presentation, is crucial for the adoption and sustained use of technology. Additionally, privacy and usability issues need to be considered in the design of mobile health systems, electronic medical records interfaces, and technology for informal caregivers and aging in place. Incorporating usability concerns alongside security is essential for the development of effective and user-friendly systems and services.

3.1 What organizations should do

Security is the measure of protection that is put in place to protect data from unauthorized access. This includes the use of encryption, authentication, and access control measures. Authentication ensures that only authorized users have access to the data. Access control ensures that only authorized users can access the data. Encryption is a process of encoding data so it cannot be read by anyone other than the intended receiver.

Privacy is the measure of ensuring that users' data is kept confidential and is not shared with anyone else. This includes the use of data privacy laws, such as the General Data Protection Regulation (GDPR), which

provides individuals with the right to know what data is collected, how it is used, and who has access to it. It also requires companies to provide users with the option to opt out of any data collection.

In order to ensure the security and privacy of users' data, organizations should implement security measures such as encryption, authentication, and access control. Additionally, they should ensure that their systems are compliant with data privacy laws and that users are aware of their rights and have the ability to opt out of any data collection.

3.2 Solutions for improving security and privacy

There are a number of solutions that can be used to improve the security and privacy of information usability. The first is improved data management policies. Businesses should implement strict policies regarding the collection, storage, and use of data. Additionally, businesses should ensure that their data is encrypted and stored securely. Another solution is the use of encryption. Encryption can be used to protect data from unauthorized access and ensure its privacy. Finally, businesses should also implement measures to detect and respond to data breaches in a timely manner.

Ultimately, security and privacy are essential aspects of information usability. Without them, users' data is at risk of being accessed and shared by unauthorized parties. By implementing the appropriate security measures and ensuring compliance with data privacy laws, organizations can ensure that users' data remains secure and private, and that their information is used appropriately.

Information security and privacy are the two major aspects of using digital information. With the rapid development of the internet and technology, it has become increasingly important to ensure that data is secure and private. In order to protect user data, organizations must have a comprehensive security and privacy policy in place.

Organizations should take steps to protect the data that they store, access, and share. This includes regularly auditing their information system and processes. Additionally, companies should ensure that their system is protected by firewalls and other types of security software that can prevent unauthorized access. Organizations should also have policies in place that dictate how data is stored, handled, and shared with other parties.

It is also important for organizations to ensure that their data is secure and private. This means that organizations should have data encryption protocols in place that protect user data. Additionally, organizations should also have authentication methods in place that require users to prove their identity before accessing sensitive information.

Organizations should also be aware of the privacy rights of their customers. They should ensure that user data is only used for the purposes that it was collected for and that it is not shared with third parties without the user's express permission. Additionally, companies should have procedures in place that allow users to access, update, and delete their personal data.

Finally, organizations should also ensure that their users understand the security and privacy measures that are in place. Companies should provide users with clear information about their security and privacy policies, as well as how to contact customer service or the organization if they have any questions or concerns.

By taking the necessary steps to ensure that their data is secure and private, organizations can ensure that their users' data is safe and secure. This will help to protect the reputation of the organization and the trust that users have in the organization. Additionally, it will also help to ensure that users have access to the information that they need in a secure and private manner.

4. Conclusion and implications for the future

Security and privacy are essential for the proper functioning of information usability. This paper has explored the current state of security and privacy in this area, including the legal and technological frameworks surrounding it, its impact on businesses and individuals, and potential solutions for improving security and privacy. Additionally, this paper has considered the implications of the current state of security and privacy on the future of information usability. As data becomes increasingly valuable, it is essential that businesses and individuals take steps to ensure its security and privacy.

The current state of security and privacy in information usability has significant implications for the future. As data becomes more valuable, businesses and individuals will need to take steps to ensure its security and privacy. Additionally, governments and regulatory bodies may need to introduce stricter regulations to protect user data. Finally, technological solutions, such as encryption and data masking, will need to be further developed and implemented to ensure the security and privacy of user data.

References

[1] Adnan, K., Akbar, R., & Wang, K. (2021). Development of usability enhancement model for unstructured big data using slr. Ieee Access, 9, 87391-87409. https://doi.org/10.1109/access.2021.3089100

[2] Gordon, J., Calabretto, J., & Sorich, M. (2011). Unanswered health-related questions in community pharmacy: frequency, nature and consequences. Journal of Pharmacy Practice and Research, 41(4), 271-274. https://doi.org/10.1002/j.2055-2335.2011.tb00102.x

[3] Harrison, R., Flood, D., & Duce, D. (2013). Usability of mobile applications: literature review and rationale for a new usability model. Journal of Interaction Science, 1(1), 1. https://doi.org/10.1186/2194-0827-1-1

[4] Nabovati, E., Vakili-Arki, H., Eslami, S., & Khajouei, R. (2014). Usability evaluation of laboratory and radiology information systems integrated into a hospital information system. Journal of Medical Systems, 38(4). https://doi.org/10.1007/s10916-014-0035-z

[5] Elers, P., Hunter, I., Whiddett, D., Lockhart, C., Guesgen, H., & Singh, A. (2018). User requirements for technology to assist aging in place: qualitative study of older people and their informal support networks. Jmir Mhealth and Uhealth, 6(6), e10741. https://doi.org/10.2196/10741

[6] Hassan, A. (2020). Challenges and recommendations for the deployment of information and communication technology solutions for informal caregivers: scoping review. Jmir Aging, 3(2), e20310. https://doi.org/10.2196/20310

[7] Irizarry, T., Dabbs, A., & Curran, C. (2015). Patient portals and patient engagement: a state of the science review. Journal of Medical Internet Research, 17(6), e148. https://doi.org/10.2196/jmir.4255

[8] Jnr, B. (2019). Validating the usability attributes of ahp-software risk prioritization model using partial least square-structural equation modeling. Journal of Science and Technology Policy Management, 10(2), 404-430. https://doi.org/10.1108/jstpm-06-2018-0060

[9] Justine, C., Prasad, R., & Thomas, C. (2018). Game theoretical analysis of usable security and privacy. Security and Privacy, 4(5). https://doi.org/10.1002/spy2.55

[10] Katusiime, J. and Pinkwart, N. (2017). A review of privacy and usability issues in mobile health systems: role of external factors. Health Informatics Journal, 25(3), 935-950. https://doi.org/10.1177/1460458217733121

[11] Liang, H., Fleming, C., & Wang, W. (2014). User authentication interfaces in mobile devices: some design considerations.. https://doi.org/10.1109/cse.2014.155

Naqvi, B., Clarke, N., & Porras, J. (2020). Incorporating the human facet of security in developing systems and services. Information and Computer Security, 29(1),

49-72. https://doi.org/10.1108/ics-11-2019-0130
[12] Yankson, B., Salgado, A., & Fortes, R. (2021). Recommendations to enhance privacy and usability of smart toys.. https://doi.org/10.24251/hicss.2021.228
[13] Zahabi, M., Kaber, D., & Swangnetr, M. (2015). Usability and safety in electronic medical records interface design. Human Factors the Journal of the Human Factors and Ergonomics Society, 57(5), 805-834. https://doi.org/10.1177/0018720815576827