

Inadvertent Disclosure Risk Behind Employee Smartphone Usage

Muhammad Usman Noor

Program Studi Manajemen Rekod dan Arsip, Program Pendidikan Vokasi, Universitas Indonesia

**) Korespondensi: usmannoor@ui.ac.id*

Abstract

The leakage of information could lead to material or immaterial losses. Information leakage occurs due to intrusion from outside parties and also due to the negligence of the information owner. Information leakage caused by the information holder referred to as inadvertent disclosure. The impact of inadvertent disclosure is riskier if it occurs in the workplace. In the workplace, confidential and sensitive information or trade secrets cannot be disclosed to the public. In practice, leakage of company information can occur because of tiny, neglected things such as accidentally uploading the information on social media or sending the information to the wrong person on a messaging application, which then brings losses or legal problems. This study uses a quantitative approach with a survey mode of data collection on 220 respondents. The results of this study indicate that most professionals have taken pictures or recorded videos while in the work area or while working; this results in the possibility of confidential information being accidentally recorded. And this confidential information access social media and messaging apps more than ten times a day. This phenomenon illustrates that a high frequency of access could increase the risk of inadvertently posting, uploading, or sending wrong photos or videos that contain confidential information that should not be disclosed. The author suggests the need for proper information governance through policy and rules following organizational culture in order to prevent accidental.

Keywords: inadvertent disclosure; information governance; social network sites; smartphone use

Abstrak

Kebocoran informasi dapat menimbulkan kerugian materiil atau imaterial. kebocoran informasi tidak hanya terjadi karena intrusi dari pihak luar namun dapat dikarenakan kelalaian pemilik informasi. Kebocoran informasi karena kelalaian sendiri disebut sebagai kebocoran informasi tidak disengaja. Dampak dari hal tersebut lebih berisiko apabila terjadi di dunia kerja. Pada dunia kerja informasi rahasia dan sensitif atau rahasia dagang adalah sesuatu yang tidak dapat dikemukakan pada publik. Pada praktiknya kebocoran informasi perusahaan dapat terjadi karena hal sepele seperti tidak sengaja unggah di sosial media atau salah kirim pada aplikasi pesan, yang kemudian membawa kerugian atau masalah hukum. Penelitian ini bertujuan untuk memahami perilaku perekaman informasi menggunakan smartphone dan frekuensi penggunaan social media dan aplikasi perpesanan dalam konteks risiko terjadinya kebocoran informasi tidak disengaja. Penelitian ini menggunakan pendekatan kuantitatif dengan mode pengambilan data secara survey pada 220 responden. Hasil penelitian ini menunjukkan bahwa Sebagian besar profesional pernah mengambil gambar atau merekam video selama berada di area kerja atau ketika bekerja, hal ini mengakibatkan kemungkinan adanya informasi rahasia yang secara tidak sengaja terekam. Dan informasi rahasia ini ada pada smartphone pribadi dari masing-masing pegawai, yang relatif sulit untuk dikontrol. Lebih jauh, sebagian besar profesional mengakses social media dan aplikasi perpesanan lebih dari 10 kali dalam sehari. Hal ini menggambarkan tingkat akses yang tinggi dapat meningkatkan risiko ketidaksengajaan posting, unggah, atau salah kirim foto atau video yang didalamnya mengandung informasi rahasia yang seharusnya tidak boleh disebarluaskan. Penulis menyarankan perlu adanya tata Kelola informasi yang tepat dan sesuai dengan kultur organisasi agar dapat mencegah terjadinya kebocoran informasi.

Kata Kunci: kebocoran informasi; tata kelola informasi; media sosial; penggunaan smartphone.

1. Introduction

Information leakage or a data leak can create significant damages to the affected parties, both material and immaterial. Information leakage occurs in individuals or organizations context, but somehow it takes a bigger loss in organization scope. Information leakage is a condition where there is information that external parties should not know, usually trade secret or secret information, but unfortunately, the information falls to external parties. The urgency of information leakage has increased sharply since the digital era, where information can be in various locations and forms and is easily accessible using the internet network. The leakage process can occur in the digital environment due to several ways, such as theft or data burglary using hacking, cracking, carding, skimming, phishing, malware, cybersquatting or wiretapping methods to gain information from the victims (Islami, 2018). However, information leakage does not only count because of the intervention of external parties who deliberately or intentionally want to obtain the information. The Information leakage can also be caused by the negligence of internal parties or the individual itself; information that should not be released but accidentally leaked coined as Inadvertent Disclosure.

Inadvertent Disclosure term describes confidential client information disclosure to opposing counsel with no intent to reveal confidential information (Schaefer, 2010). Inadvertent disclosure often occurs due to the carelessness, ignorance or unintentional of the perpetrator. The chance to inadvertent disclosure is getting easier and riskier now because of the ease of recording information via smartphones. It does not stop there; the ease of disseminating information through various channels such as social media or messaging applications are also increasing the risk of inadvertent disclosure. By now, social media is a “favourite” location for accidentally uploading documents in various forms such as photos, videos, PDFs, or compressed files that contain confidential information in those items (Rubell, 2017; Schaefer, 2010). A greater loss caused by inadvertent disclosure in material and immaterial is more harmful if it occurs in a professional scope, such as a company, organization or government. As mentioned by Flynn (as cited in (Kluemper et al., 2016) in general, staff or employee participation and engagement in social media reputational damage, trigger lawsuits, cause humiliation, crush credibility, destroy careers, create electronic business records, and lead to productivity losses. The personal social media account from the employee is the spotlight in this case. A higher frequency of using social media leads to a greater chance of inadvertent disclosure, so the risk also spikes. Furthermore, this matter could not be taken lightly and become a matter.

The COVID-19 pandemic has also prompted changes in our daily life, including work behaviour in many ways. The Work from Home (WFH) term becomes a common norm and widely applied to many industries that possible to work remotely from home. In Indonesia more than 65% employees started . This change leads to a drastic change in how people see the working place. Working cubical turns out to be a dinner table, and a meeting room in our living room has become common. This changing behaviour leads to dissipating boundaries between public and private work areas because it is hard to distinguish

between them. Changes in the work environment from the office to home have resulted in higher frequency to access their smartphone or laptop due to the need to stay connected with colleagues or supervisors. This phenomenon prompts someone to be more careless and unaware of documents that contain secret or sensitive information that should not be disclosed.

This study aims to explore and understand the behaviour of recording information using a smartphone and the frequency of accessing social media and messaging applications. The bigger picture then analyzes to understand deeper about the risk of inadvertent disclosure that can occur in the work environment. Hopefully, this study could raise public awareness about the risk of inadvertent disclosure. The organization or company could respond to create a more appropriate and effective information governance policy to prevent inadvertent disclosure in theirs.

2. Previous Findings

Inadvertent Disclosure term describes a disclosure of confidential client information to opposing counsel with no intent to reveal confidential information(Schaefer, 2010) in a broader way. It could be an accidental exposure of information to a person not authorised access(National Institute of Standards and Technology, 2020). In the past, inadvertent disclosure happens when in large document processed on a screening procedure, the privileged document can easily slip through into adversaries hand. Moreover, this problem has become increasingly common as litigation and document production grow in size(Michigan Law Review, 1983). Into newer context, in the digital information era, inadvertent disclosure can be received through various forms, e.g. photo and video sharing on the social media, misdirected e-mail, confidential information embedded on the document metadata, a protected document mistakenly included in release document(Rubell, 2017; Schaefer, 2010). related to any business information, not only related to a legal document, and the scope including new technologies, including the internet and Web 2.0 application.

SNS also can be a perfect place to accidentally shared confidential information. Some example of inadvertent disclosure on SNS are Workplace Posts Can Lead to Data Leakage; Geo-Location tracking; Collaborative Contract; and Language Limitations(Gillman et al., 2018). Inadvertent Disclosure on the SNS could be classified as security incidents or violation of information security because one the component which is information has been disclosed to an unauthorised person has been violated(Keyser & Dainty, 2016) in another hand it could be led to massive setback such as a loss of competitive advantage, loss of reputation, and erosion of client trust(Abdul Molok et al., 2018).

3. Method

This study uses a quantitative approach; this study seeks to see phenomena related to the understanding of inadvertent disclosure risk by examine the participant experience in taking document using smartphone in their workplace and social media or chat application usage in workdays. The data used in the research was obtained by using an online questionnaire method. The online questionnaire was given

randomly to workers who work in various fields, the respondents being in the age range of 20 to 60 years. Respondents in this study consisted of 220 professionals/workers who worked as Civil Servants, Private, and State-Owned Enterprises (BUMN). Respondents came from various major cities in Indonesia, including Greater Jakarta, Bandung, Surabaya, Medan, Semarang, Pontianak, and Lampung. The online questionnaire was distributed through various social media to respondents were randomly obtained from various cities in Indonesia. The online questionnaire collection period conducts from December 2020 until May 2021.

This research used descriptive analytic method to illustrate and describe the collective data to draw conclusions (Sugiyono, 2014). Some of the variables that will be discussed in this study include the experience of taking pictures or photos and recording videos while in the work environment and during working hours. As a note, in this study, the home area is used as a work area when the respondent used a WFH scheme. In addition, it also discussed the frequency of respondents in accessing messaging applications such as WhatsApp, LINE, Telegram or similar and social media such as Instagram, Twitter, and Facebook.

4. Result And Discussion

Inadvertent disclosure can occur from the smallest extent, which is started by the individual. Generally speaking, inadvertent disclosure occurs in the individual circle, but the loss could be hit into organizational scope. The inadvertent disclosure rarely happens at the collective level since it usually happens because of the individual's negligence. Thus it is necessary to deeply understand the context of these behaviors from the most basic level, from each individual. In an inadvertent disclosure context, the most important thing is the information itself. The information is only possible to communicate or disseminate when recorded in various forms and formats, such as text, sound, images, and moving images; if not, the information only circles on the people head and becomes tacit knowledge.

Documents, records, photos and videos are the output of the recording process. All the process could be done by only using our smartphone. Hence, it is necessary to pay attention to the flow and distribution traffic of the records created by that process. If a person never records the information, certainly, the information will never be disseminated unless the person knows the information disseminates it orally spoken. Vice versa, if the information is recorded in any forms and formats mentioned above, no matter how tiny they are, there is still the possibility that the information will be disseminated, either intentionally or unintentionally. With the almost all smartphones that we use today can record information in various forms; the ability to take pictures and videos, sound. Some of the latest smartphones even attached with light sensors can take the geometry of artefacts or objects into 3D files, such as iPhone 12 Pro that featured a LIDAR scanner. Our convenience in recording information using smartphones is certainly an advantage in itself, but we need to understand that there is a risk of inadvertent disclosure behind it.

The questionnaire results show that 94% of the workers surveyed indicated having taken pictures using a smartphone while in their work environment, as shown below.

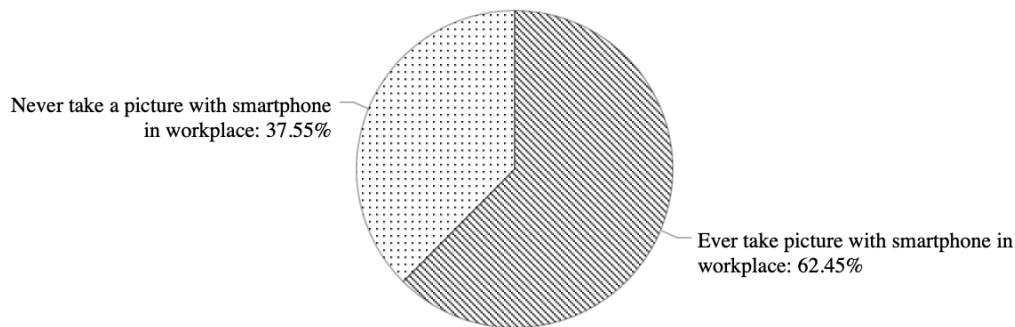


Table 1 Experience in taking picture in Workplace Area

Source: Research Dataset

This data shows that almost all professionals or workers have taken pictures in the work environment using their cellphones; this is not surprising given the ease of taking pictures using a smartphone. More than 40% of participants admit that they have taken pictures while working with colleagues, such as during meetings, formal activities in the work environment, meetings, events held in groups in the office. At first glance, it seems harmless, but there is no guarantee that there is no fragment or piece of secret or sensitive information not included in those pictures.

For example, a photo in a meeting room can contain information on a whiteboard that should, for example, not be known to external parties. Not only organizational information that can be recorded, information about personal data or personal information about our co-workers can also be recorded, among others, real names, identity numbers, photos or videos of co-workers' faces. Maybe some people do not think of this as personal information. However, from previous research, it was found that many people feel that uploading photos, videos that contain themselves without consent are part of a violation of their privacy. Furthermore, many of them consider that information such as full name, identity number is part of their personal information that should not be disseminated (Noor, 2020).

In addition, when they are working with colleagues, respondents also often take pictures while doing work independently. As many as 35% of respondents have taken pictures while working independently, and the objects taken by some of them are very risky to contain information that should not be released, such as documents or archives being worked on. Although the employee may take a photo of the document for reporting purposes to his boss or co-worker and does not want to post it on the internet, there is no guarantee that the photo will be deleted immediately. Moreover, there is a risk of accidentally posted on social media or sent to the wrong place on a messaging application such as Whatsapp or LINE. A messaging

application such as Whatsapp, LINE or telegram, is needed to accommodate the communication to his co-worker and complete the task. However, this increases the risk of inadvertent disclosure in the messaging application. From the application security views, these applications are generally safe from third-party hacks because they use end-to-end encryption and certain protocols(Rahim et al., 2018). However, there is no guarantee of information leakage due to human error. This matter becomes crucial, and we need to understand human behaviour behind this to minimize the risk. The work from home lifestyle also blurred the boundaries between private life and professional work, the employee found it were not easy to distinguish the work and life related problem. Based on Li and Yuanresearch, this could lead employee to suffer work-life conflict.

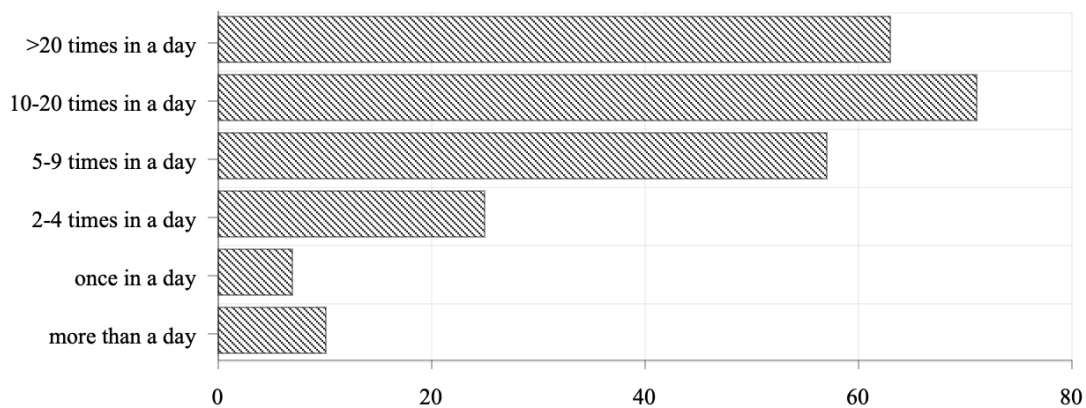


Table 2. Social Media usage Frequency

Source: Research Dataset

The data above shows that the use of social media from workers who are respondents in the study is very high. Approximately 55% of respondents access social media such as Facebook, Instagram, Twitter more than ten times. Seeing this data means that it is very risky for the possibility of ID in the work environment; this is in line with the high frequency of using social media in workers' daily lives. In addition, most of us upload and share information about our daily lives on social media(Venugopal, 2018), not only in daily life but also in work-related matters. The more dependence the employee with their smartphone, it seems to lead to the symptoms such as anxiety and uncontrollable usage behaviour(L. Li & Lin, 2019). Uncontrollable usage behaviour definitely could lead to uncontrolled information sharing from the subject. Even more the nature of social media was driven by the hormones of young adults who loves to express their views, facets and their life in social media, including their daily routines in the workplace. It is coherent with Robayo-Pinzon et al research, it shows the usage time of using social media and apps had a positive effect on the impulsive behaviour, this finding show the risk of people to impulsively shared something on the social media even greater.

The problem reduce the risk of inadvertent disclosure is because many of employee think their smartphone is already become part of them. They have physical proximity, constant connectivity, and customization with their smartphone and application on its. Creating such a bond between self and machine. This phenomenon create a such tricky and complicated things to create a balance policy to reduce the risk of inadvertent disclosure in workplace context. Several things that can be done to prevent accidental disclosure in the work environment can be done by implementing appropriate information governance. Information governance itself is a series of rules or policies to ensure that information is available when needed but still ensures its security. Employees and control of the organization and access to information. Furthermore, Willis(2005) suggests that there are six components in information governance in organizations, among others, transparency, accountability, legal process, compliance, applicable legal rules, and corporate and individual information security policies. Lomas(2010) argues that information governance policies rely on records and information management practices in an organization. One of the standards that can help formulate information governance in organizations is to map out a policy framework based on related international standards, such as ISO 27001 and ISO 15489 related to the organizational context. Organizations need to understand the organizational culture and applicable business processes to establish governance policies that are appropriate to the scope of work and organizational culture.

5. Conclusion

One of the technological disruptions that have occurred is the ease of recording information and disseminating information via the internet, which has driven a lot of progress and convenience in the professional sphere. However, it should be realized that there are risks that most have not been discussed in the industry, such as inadvertent disclosure. Inadvertent disclosure can occur in various information channels, one of which is social media or messaging applications from personal accounts of staff or employees of an organization. The results showed a high tendency in the context of employees to produce archives or documents in the form of photos or videos. In addition, the results of the study indicate a high frequency of employees accessing personal social media and messaging applications during working hours. The high of the two variables above increases the risk of unintentional disclosure of information.

Solutions such as banning these behaviours are certainly not wise because organizations cannot deny the benefits of implementing these technologies. In addition, technically, the company cannot monitor all information produced or disseminated. So it is necessary to have limits or applicable rules regarding information governance in the company. One thing to note is that the policy must still pay attention to the balance between the interests of the company and the protection of the employees' privacy. This research is limited by not discussing examples of accidental disclosures in the real world and how high the correlation between the two variables in this study with cases of unintentional disclosure of information that occurred in the real world can certainly be an interesting thing to study further.

Reference

- Abdul Molok, N. N., Ahmad, A., & Chang, S. (2018). A case analysis of securing organisations against information leakage through online social networking. *International Journal of Information Management*, 43(September), 351–356. <https://doi.org/10.1016/j.ijinfomgt.2018.08.013>
- Badan Pusat Statistik. (2020). *Perilaku Masyarakat di Masa Pandemi COVID-19 : Hasil Survei Perilaku Masyarakat di Masa Pandemi COVID-19* (Vol. 19, Issue September).
- Gillman, F., Thompson, B., & McCormick, S. (2018). *United States : Social Media And The Workplace – Why And How*. Lewis Brisbois Bisgaard & Smith LLP. <https://www.mondaq.com/unitedstates/employee-rights-labour-relations/754726/social-media-and-the-workplace-why-and-how-employers-should-limit-the-use-of-social-media-in-the-workplace>
- Islami, M. J. (2018). Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index. *Masyarakat Telematika Dan Informasi : Jurnal Penelitian Teknologi Informasi Dan Komunikasi*, 8(2), 137. <https://doi.org/10.17933/mti.v8i2.108>
- Keyser, T., & Dainty, C. (2016). *The Information Governance Toolkit – Data Protection, Caldicott, Confidentiality* (Vol. 20, Issue 8). CRC Press. <https://doi.org/10.7748/ns2005.11.20.8.36.b390>
- Kluemper, D. H., Mitra, A., & Wang, S. (2016). Social media use in HRM. *Research in Personnel and Human Resources Management*, 34, 153–207. <https://doi.org/10.1108/S0742-730120160000034011>
- Li, J., & Yuan, B. (2018). Smartphone Intrusion: Has Social Interaction Online Blurred the Work–Life Boundary of Employees? *Cornell Hospitality Quarterly*, 59(4), 411–427. <https://doi.org/10.1177/1938965518777217>
- Li, L., & Lin, T. T. C. (2019). Smartphones at Work: A Qualitative Exploration of Psychological Antecedents and Impacts of Work-Related Smartphone Dependency. *International Journal of Qualitative Methods*, 18, 1–12. <https://doi.org/10.1177/1609406918822240>
- Lomas, E. (2010). Information governance: Information security and access within a UK context. *Records Management Journal*, 20(2), 182–198. <https://doi.org/10.1108/09565691011064322>
- Michigan Law Review. (1983). Inadvertent Disclosure of Documents Subject to the Attorney-Client Privilege. *Michigan Law Review*, 82(3), 598–624. <https://doi.org/10.2307/1288648>
- National Institute of Standards and Technology. (2020). *Computer Security Resource Center Glossary*. https://csrc.nist.gov/glossary/term/system_owner
- Noor, M. U. (2020). Indonesian millennial awareness to privacy and personal data protection on the internet. *DESIDOC Journal of Library and Information Technology*, 40(2), 431–436. <https://doi.org/10.14429/djlit.40.02.14969>
- Park, C. S., & Kaye, B. K. (2019). Smartphone and self-extension: Functionally, anthropomorphically, and ontologically extending self via the smartphone. *Mobile Media and Communication*, 7(2), 215–231. <https://doi.org/10.1177/2050157918808327>
- Rahim, R., Siahaan, A. P. U., Manikandan, R., Aryza, S., Kurniasih, N., Djanggih, H., Prawira Buana, A., Moonti, R. M., & Riswanto, A. (2018). Insecure Whatsapp Chat History, Data Storage and Proposed

- Security. *International Journal of Pure and Applied Mathematics*, 119(16), 2481–2486.
- Robayo-Pinzon, O., Foxall, G. R., Montoya-Restrepo, L. A., & Rojas-Berrio, S. (2021). Does excessive use of smartphones and apps make us more impulsive? An approach from behavioural economics. *Heliyon*, 7(2), e06104. <https://doi.org/10.1016/j.heliyon.2021.e06104>
- Rubell, P. (2017). *Disclosure of Corporate Information Through the Use of Social Media: Identifying the Risks and Adopting Best Practices*. http://www.academia.edu/4842241/Disclosure_of_Corporate_Information_Through_the_Use_of_Social_Media_Identifying_the_Risks_and_Adopting_Best_Practices
- Schaefer, P. (2010). *The Future of Inadvertent Disclosure: the Lingering Need to Revise Professional Conduct Rules*. 69(2).
- Sugiyono. (2014). *Metode Penelitian Pendidikan Pendekatan Kuantitatif, Kualitatif, dan R&D*. Alfabeta.
- Venugopal, A. V. (2018). Inadvertent disclosures of inventions in social media affecting patent rights. *Computers and Security*, 72(January 2017), 136–144. <https://doi.org/10.1016/j.cose.2017.09.007>
- Willis, A. (2005). Corporate governance and management of information and records. *Records Management Journal*, 15(2), 86–97. <https://doi.org/10.1108/09565690510614238>