12-15-2019

Privacy violations in light of digital transformation: insights from data breaches in Norway

Leif Skiftenes Flak

Øystein Sæbø

Paolo Spagnoletti

Privacy violations in light of digital transformation: insights from data breaches in Norway

Leif Skiftenes Flak
Department of Information Systems, University of Agder,
Kristiansand, Norway

Øystein Sæbø
Department of Information Systems, University of Agder,
Kristiansand, Norway

Paolo Spagnoletti[1]
Department of Information Systems, University of Agder,
Kristiansand, Norway

ABSTRACT

Privacy violations are an important unintended consequence of digitalization. Privacy and security have been studied within single, or a limited set of, organizations thus providing only a limited perspective of the nature of the phenomenon. Further, emerging technology developments related to platforms, IoT and big data may introduce new threats to security and privacy. In this paper we analyse 835 records of privacy violations in Norway. This allows us to report on the nature and consequences of privacy violations from a large number of cases based on a rich and current set of data. We apply a sequential mixed-method to explore the data set and theorize on the impact of digitalization on privacy. Our research contributes to an improved understanding of security and privacy concerns associated with digitalization.

Keywords: privacy; digitalization; data breach; GDPR; mixed-method

INTRODUCTION

While digitalisation creates a myriad of benefits for individuals, organisations and societies and actually reshapes human life, these benefits come with a price. Social media, smart phone, apps and position-based services simplify our lives, while digitalization also puts at risk

[1] Corresponding author. paolo.spagnoletti@uia.no +39 347 3123560

the privacy of our data as we rely on organizations that become victims of data breaches. A data breach is the unintended access to personal data and a major type of privacy violation (Culnan and Williams 2009). A data breach may be caused by phishing, hacking and other attacks or by accidental actions (Goode et al. 2017; Khan et al. 2019). Whenever these private data are not properly protected, unauthorized access to them may harm individual users and generate financial losses to service providers (Goode et al. 2017; Khan et al. 2019). Moreover, emerging trends in digital technologies (e.g. platforms, IoT and big data) can potentially introduce entirely new security threats that can lead to large-scale privacy violations (e.g. Goode et al. 2017).

From a regulatory perspective, privacy control is a key concern for organizations managing personal data. For instance, within the European Union, every organisation, regardless of size, sector or service provided, has to comply with the General Data Protection Regulation (GDPR[2]). Implemented in 2018, the GDPR aims primarily to give control to individuals over their personal data by imposing legal obligations to companies managing their data. Controllers of personal data must put in place appropriate technical and organisational measures to implement the data protection principles. Moreover, organizations must send a notification of data breaches to a supervisory authority and, in some cases, to the (affected) public. The notifications of data breaches provide a systematic feedback about the actual risk and the weaknesses of existing security measures. On one side, data breach notifications are expected to foster mutual learning, public awareness and self-improvement for privacy protection (Porcedda 2018). On the other side, the company reputation is threatened by perceived responsibility and attribution of data breaches that can be determined by ethical misdemeanor, poor controls, and weak governance structures (Syed 2018).

[2] The European Data Protection Regulation (2016/679) is applicable as of May 25th, 2018 in all member states to harmonize data privacy laws across Europe.

Previous works have, to a large extent, focused either on causes, locus or impact of data breaches (Khan et al. 2019; Garrison and Ncube 2011), with the aim of enhancing organizational privacy programs (Culnan and Williams 2009). For instance, factors influencing the risk of privacy violation have either investigated data breaches at organizational level (Sen and Borle 2015; Wall et al. 2016) or at individual-employee level (Abidin et al. 2019; Canhoto 2009). Although these efforts have contributed to improve internal control systems, more research is needed to provide managers of public and private companies with analytical instruments for understanding privacy violations in light of digital transformation.

In this paper we develop a conceptual framework of privacy violations based on the analysis of a rich set of data breach information. The nature of data breaches will be analysed in light of the digitalisation trends affecting both business and criminal communities. The organizing logics of digital innovation (Yoo et al. 2010) are in fact transforming also the cybercrime business, resulting in new forms of cyber-attacks (Huang et al. 2018) that make obsolete the traditional categories of information security incidents (Baskerville et al. 2014). Our empirical analysis is based on a rich dataset of all reported privacy violations occurring in Norway over a period of 6 months in 2019. Further, we analyse a selection of decision letters since the introduction of GDPR. This way, we contribute to an improved understanding of security and privacy concerns associated with digitalization by exploring the links between technologies, policies, processes, society, economy and legislation as suggested by Lowry et al. (2017). Moreover, our focus on organizational-level privacy violations allows us to contribute to the development of adequate mitigation mechanisms.

In Norway, privacy violations are handled by the Norwegian Data Protection Authority (NDPA). Since the introduction of GDPR, the number of reported privacy violations has

increased dramatically. These reports on data breaches are submitted by the organizations where the violations occurred and contain detailed information about e.g. the nature of the violation, the sector in which it occurred, number of affected people, the cause of the violation and potential consequences of the violation. NDPA considers each report and can issue reactions in cases where organizations have not acted in accordance with GDPR. In cases of potential GDPR negligence, NDPA conducts an investigation of the case and summarizes the case and outcome of investigation in a decision letter. We have access to 835 data breach reports and decision letters of cases where NDPA has concluded that GDPR has been violated. This rich data set provides an extensive basis for exploring, understanding and theorizing around organizational privacy violations as one of the dark sides of digitalization.

We conduct a mixed method explanatory design, involving the collection and analyses of quantitative and qualitative data in two consecutive phases (Ivankova et al. 2006). We do so to provide rich and deep insights into the phenomena at hand (data breaches and digitalization), to expand our knowledge on the dark side of digitalisation. The sequential explanatory design implies that qualitative data is collected to help explaining or elaborating quantitative results (Venkatesh et al. 2013, 2016). Our first step consists of conducting a quantitative analysis of the 835 reported data breaches received by NDPA. The study of numeric data in the first phase provides us with a broad and general understanding of the research problem (Ivankova et al. 2006). The next step includes a qualitative analysis of both secondary and primary data. We perform a content analysis of decision letters, presenting the result of the investigations by the NDPA on a number of cases involving the violation of the GDPR regulations. These letters provide us with a more in-depth description, extending our understanding of the phenomena. Then, we complete the qualitative part of our mixed method explanatory design by conducting

interviews with privacy experts who have been involved in processing the data breach data. Inspired by Ivankova et al. (2006) our preliminary research design is visualised in Figure 1.

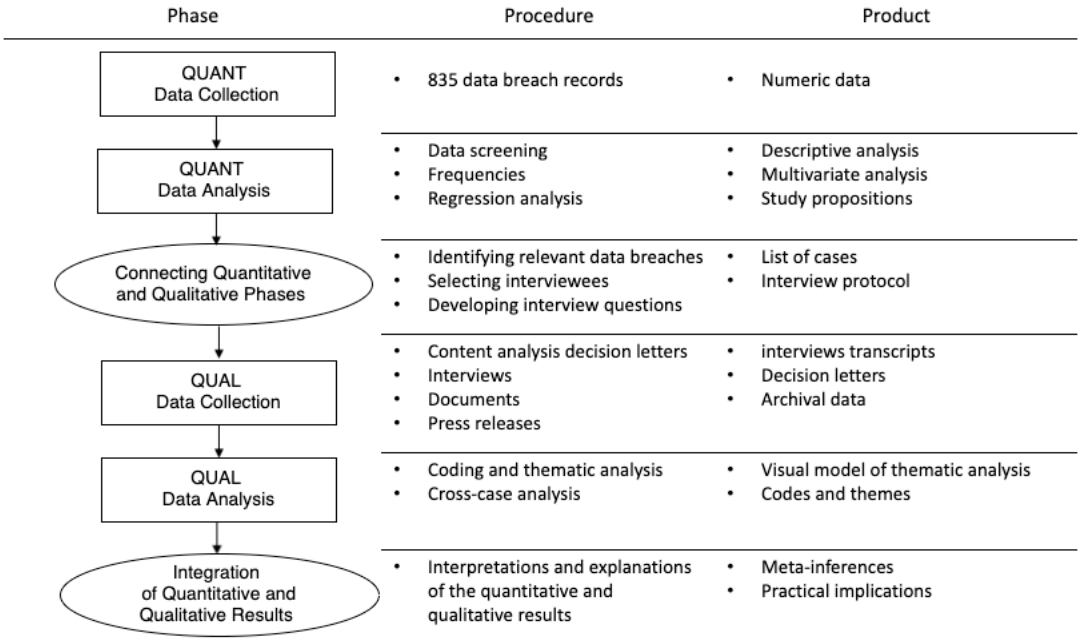

Figure 1. Research design

REFERENCES

Abidin, M. A. Z., Nawawi, A., and Salin, A. S. A. P. 2019. "Customer Data Security and Theft: A Malaysian Organization's Experience," *Information and Computer Security* (27:1), pp. 81–100.

Baskerville, R., Spagnoletti, P., and Kim, J. 2014. "Incident-Centered Information Security: Managing a Strategic Balance between Prevention and Response," *Information & Management* (51:1), Elsevier B.V., pp. 138–151.

Canhoto, A. I. 2009. "Safeguarding Customer Information: The Role of Staff," *Journal of Consumer Marketing* (26:7), pp. 487–495. (https://doi.org/10.1108/07363760911001547).

Culnan, M. J., and Williams, C. C. 2009. "How Ethics Can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches," *MIS Quarterly* (33:4), pp. 673–687.

Goode, S., Hoehle, H., Venkatesh, V., and Brown, S. A. 2017. "User Compensation as a Data Breach Recovery Action: An Investigation of the Sony Playstation Network Breach," *MIS Quarterly* (41:3), pp. 703–727.

Huang, K., Siegel, M., and Madnick, S. 2018. "Systematically Understanding the Cyber Attack Business: A Survey," *ACM Computing Surveys* (51:4), pp. 1–36.

Ivankova, N. V, Creswell, J. W., and Stick, S. L. 2006. "Using Mixed-Methods Sequential Explanatory Design: From Theory to Practice," *Field Methods* (18:1), Sage Publications Sage CA: Thousand Oaks, CA, pp. 3–20.

Khan, F., Kim, J. H., Moore, R., and Mathiassen, L. 2019. "Data Breach Risks and Resolutions: A Literature Synthesis," in *Twenty-Fifth Americas Conference on Information Systems, Cancun*, pp. 1–10.

Lowry, P. B., Dinev, T., and Willison, R. 2017. "Why Security and Privacy Research Lies at the Centre of the Information Systems (IS) Artefact: Proposing a Bold Research Agenda," *European Journal of Information Systems* (26:6), pp. 546–563.

Porcedda, M. G. 2018. "Patching the Patchwork: Appraising the EU Regulatory Framework on Cyber Security Breaches," *Computer Law and Security Review* (34:5), Elsevier Ltd, pp. 1077–1098. (https://doi.org/10.1016/j.clsr.2018.04.009).

Posey Garrison, C., and Ncube, M. 2011. "A Longitudinal Analysis of Data Breaches," *Information Management & Computer Security* (19:4), pp. 216–230.

Sen, R., and Borle, S. 2015. "Estimating the Contextual Risk of Data Breach: An Empirical Approach," *Journal of Management Information Systems* (32:2), Routledge, pp. 314–341.

Syed, R. 2018. "Enterprise Reputation Threats on Social Media: A Case of Data Breach Framing," *Journal of Strategic Information Systems* (28:3), Elsevier, pp. 257–274.

Venkatesh, V., Brown, S. A., and Bala, H. 2013. "Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems," *MIS Quarterly* (37:1), pp. 21–54.

Venkatesh, V., Brown, S. A., and Sullivan, Y. W. 2016. "Guidelines for Conducting Mixed-Methods Research: An Extension and Illustration," *Journal of the Association of*

Information Systems (17:7), pp. 435–495.

Wall, J. D., Lowry, P. B., and Barlow, J. B. 2016. "Organizational Violations of Externally Governed Privacy and Security Rules: Explaining and Predicting Selective Violations under Conditions of Strain and Excess," *Journal of the Association of Information Systems* (17:1), pp. 39–76.

Yoo, Y., Henfridsson, O., and Lyytinen, K. 2010. "The New Organizing Logic of Digital Innovation: An Agenda for Information Systems Research," *Information Systems Research* (21:4), pp. 724–735.