Aalto University
School of Business

THE IMPACT OF BIG DATA ON CUSTOMER DATA PRIVACY AND SECURITY

What customer data privacy and security challenges emerge from big data use and how to mitigate them

Bachelor's Thesis
Lauri Wikberg
Aalto University School of Business
Information and Service Management
Spring/Fall 2023

Aalto University
School of Business

Aalto University, P.O. BOX 11000, 00076 AALTO
www.aalto.fi

Abstract of Bachelor's thesis

Author Lauri Wikberg

Title of thesis The Impact of Big Data on Customer Data Privacy and Security

Degree Bachelor's degree

Degree programme Information and Service Management

Thesis advisor(s) Seongtae Kim

Year of approval 2023 **Number of pages** 19 **Language** English

Abstract

(NOTE: IN THIS THESIS CONTEXT CUSTOMER IS A SYNONYM FOR CONSUMER)

Global digitalization has disrupted our understanding of information in the web. Data poses a source for efficiency which brings numerous business possibilities. In recent decades, we have seen an exponential rise in the stream of consumer unstructured data with different characteristics such as velocity, volume and variety. In order to utilize this data to firms' business purposes, firms have needed to increase their investments and innovate new business models.

Challenges regarding the big data often rise from the infrastructure needed to handle the vast amount of data, but also from the framework of fair information practices (FIP). The customers' awareness of their data has improved drastically and legislation measures are being improved. Thus, there is a value proposition to give in exchange to customers' data and it is often as simple as to keep good care of it.

This thesis will be a literature review on customer data privacy and security amid big data. Thesis aims to examine what customer data privacy and security concerns rise from utilizing big data and advancements in IT, and how companies can alleviate those concerns. Thesis will also investigate boundary turbulence phenomena in business situations where customers' expectations are not met, what are their causes and consequences. A case study on Facebook data breach is also conducted.

Keywords customer data, data privacy, data security, big data

Table of Contents

1 Introduction

The advancements in information technology (IT) in every area of society, particularly Internet of Things (IoT), have generated enormous amounts of data from individuals' behavioural patterns and hence created a possibility for an effective customer identification. The availability of big data combined with effective tools for analytics is becoming a key source for competitive advantage in firms' operating environment. Big data have estimated to generate $610 billion in annual economic gains regarding productivity and cost savings (Kshetri, 2014). However, the utilization of big data in data-driven-decision making (DDDM) does not come without issues. Customers' data privacy and security concerns are a major issue to be solved.

The problem is not straightforward because customers often individually form their disposition to value privacy (DTVP) (Xu et al., 2011), However, the consequences of hypothetical data breaches are still often felt evenly severely between individuals regardless of their DVTP. The control of the data is in the hands of firm, making the firm responsible of it in the end. Hameed et al., (2012) argues that the entire society should form boundaries on what customer data should not be disclosed and to what extent customers' privacy should be respected.

The rapid evolution and innovations in IT have made privacy the most important issue for customers doing business with firms associated with information technology (Hameed et al., 2012). Customers are nowadays more aware of their data and the privacy and security concerns associated with it. Hameed et al., (2012) points out that surveys have indicated customers' concerns of firms' lack of honesty and misuse regarding to their disclosed information. The concerns are not something to be ignored as the consequences of personal information misuse can cause huge financial and emotional pain to the individuals that are victims of data breach. Those misuses can be identified as identity theft, financial fraud and numerous other threats that collectively costs of millions of dollars yearly for individuals, firms and government (Hameed et al., 2012).

Firms' intra operations call for professionals to intercept the data, and investments in up-to-date systems. By big data's nature, intercepting it requires efficient computing power to manage the operations. Therefore, firms have started to utilize cloud computing and non-relational data bases. Non-relational data bases largely construct of unstructured data which needs to be utilized with more advanced privacy aware access

control (PAAC) measures in mind (Colombo & Ferrari, 2015). Cloud computing also poses a threat for customer data security as the volumes are large and outside of the firm's walls. This gives co-control of the data to the cloud service providers who might then mismanage its responsibilities. The complexity of network among other different cloud computing service providers for firms also creates a large surface for cyber attacks (King & Raja, 2012). Apart from technical challenges, firms also need to make sure that they obey to regulations and communicate their intentions of use with the customer data authorizing the secondary use of data. As Libaque-Saenz et al., (2016) points that organizations information practices may have an influence on customers' willingness to do business with them and authorize the use and collection of private information. Studies have shown, that failing to meet customers' expectations will greatly affect the firm's reputation and thus performance (Martin et al., 2017). Moreover, it is not about the actual data misuse, but rather the vulnerability of potential misuse. This highlights the importance of firms' data management policies to be transparent.

The literature reviewing the collective interaction between customers and firms regarding customer data privacy and security have been somewhat little. The literature mainly focuses on how customers form privacy concerns opposed from how these concerns translate to actions and consequences. Consequently, in the era of digitalization and the unprecedented stream of big data, it is important to review what are the challenges that are looming. The aim of this thesis is to shed light to challenges regarding to this topic and find the overall link on how customers perceive the trustworthiness of firm and hence decide to do business with. This thesis examines measures on how firm can alleviate those trust concerns to establish a sustainable customer relationship, even in the event of data breach. Thesis will analyse the phenomena mainly through two theories: communication privacy management theory and situational crisis communication theory. A relationship marketing theory alongside with the resource-based view framework will be used as a supplementary to validate the firm's efforts in encouraging responsible data management activities.

1.1 Research objectives and research questions

The objective of this thesis is to examine what factors influence customers intentions to do business with a firm that collects, analyses and monetizes customer data, and how a firm can reassure its existing and potential new customers on responsible and ethical data management. Thesis will also discuss about the challenges regarding intercepting big data and what consequences mismanaging the customers' data has. Through utilizing existing literature, thesis will provide insights into dynamics of this phenomena. In a digital world, a better understanding of how firms should manage its data and policies regarding to customers' privacy and security concerns is the goal of this thesis. A case study of Facebook (Meta) will be used for a real-life example to give credibility to thesis.

Specific research questions in this thesis are:

(1) How heightened customers perceptions of firm's data privacy and security measures affect the customers intentions to disclose information?

(2) What are the challenges regarding customer data privacy and security to firms amid big data and how these challenges can be alleviated?

With these questions and previously mentioned theories and framework in mind, thesis reviews the current challenges associated with the topic.

1.2 Scope of research

The scope of this thesis is mainly focused on firms' data privacy and security measures and actions, perceived and interacted by customers thus affecting firms' operations handling the big data. Thesis will be a literature review with number of journal articles and studies examined, weighting recent findings.

There are a number of limitations to this thesis. First, this thesis does not cover the differences in legislation across continents, even though the transmitting of the data is often exceptionally global. Second, the thesis does not aim to do an exhaustive analysis of every single factor affecting the dynamic between the customers and firms, but rather aims to bring an overview of the key concepts and challenges associated with the relevant overall issues of the topic. Different legislations, for example GDPR in Europe sets a strict framework to investigate and that could be another fruitful study to conduct.

1.3 Methodology

This thesis is a descriptive analysis of the topic, utilizing the recent relevant literature to answer what are the challenges in the complex digital business environment regarding to the research questions. Literature review is chosen due to the complexity and of the qualitative nature of the topic. More advanced methods could give different fruitful insights.

The main sources for gathering the literature were Scopus and Google scholar, with keywords used such as: “data privacy”, “data security”, “big data” and “customer data”. The criteria for articles used in this thesis are inspected carefully to satisfy the relevant field as well as being recent as the technology have accelerated quickly thus changing the landscape rapidly. Authors are checked for validity and articles with higher citations were prioritized. The criteria of recently published journals is more relaxed when inspecting the dynamic how customers make decisions to or not to disclose information with any firm. This is because such decision-making process is more about the nature of people. Nevertheless, the insights of the literature in this aspect as well are taken into the context of concerns today as regarding big data.

The research questions are investigated with a problem – solution approach, with a case study highlighting the importance of the “solution” part of the equation. After carefully examining the articles, we are left with 11 articles to citate and to answer to the research questions. Two (2) newspaper articles were also used.

1.4 Structure of the research

The rest of the thesis is structured as follow. Chapter 2 reviews the background of the topic and theoretical frameworks used to conduct this thesis. Chapter 3 will be divided into two sub chapters to answer the outlined research questions as follows. The first sub chapter will examine customers' perception of firms' ability to securely and privately handle disclosed customer data and hence, at what terms customer is willing to do business with the service providers (i.e disclose information). The second sub chapter examines how firms' can respond to challenges regarding to customers' concerns of their data and optimize their intra operations to obey with the expectations. Studies of the effects of failing to meet privacy and security expectations in the form of boundary turbulence will be examined. In chapter four, a case study of Facebook's 2018 turbulence is used to showcase practical effects of a violation towards customers' trust to give credibility and additional clarity to the thesis. Facebook is chosen for the case study due to its popularity, influence and being one of the first platforms to effectively mine its user data.

Chapter five will conclude the thesis with discussions and conclusions of the reviewed topic, as well as discussion of the implications and limitations of the thesis. Finally, there will be a careful consideration of the limitations and some future research possibilities.

2 Theoretical background

In this chapter we will briefly go through the theoretical background of the topic and discuss the theories and framework which is used in conducting this thesis.

2.1 Theories and framework

Theoretical background of thesis' topic is based on the anxiety of risen vulnerabilities on customer's personal data misuse in digital era and thus, firms' reassure responses.

Two main theories used are communication privacy management theory and situational crisis communication theory. Communication privacy management theory highlights boundaries in which customers choose to or not to disclose their private information. Situational crisis communication theory inspects the firm's methods and strategies of response to shareholders and customers and their effectiveness in the case of crisis such as data breach. By utilizing these theories, thesis aims to find answers to the research questions. Additionally, utilizing supplementary theory and framework thesis aims to tie and validate the relationship and importance between the customers and firms trust and resource allocation.

Supplementary theory and framework used in this thesis are relationship marketing theory and resource-based view. Relationship marketing theory highlights the dynamic between value brought to customer and sustainable customer relationship and is used to validate the importance of firm's trustworthiness and hence customer retention. Resource based view is then used to determine the strategic resources a firm can use and allocate to gain sustainable competitive advantage in regard to data privacy and security in the complex digital business field, where competition for big data innovation is apparent.

3 Data privacy and security amid big data

In this part of the thesis, we will first clarify on what terms customers make decisions to interact with a firm that collects, stores, analyses and uses customer data and how it is related to the value that the service deliveries to the customer. In the second sub chapter we will examine firms' responses and measures to data privacy and security concerns, what challenges it includes and how customer can be reassured that his or her sensitive data is handled properly.

3.1 Heightened data privacy and security concerns

Heightened privacy and security concerns are intrinsic to advancements in IT, and they need to be considered. By big data's nature of collecting, storing, analysing and using enormous amounts of personal data, it has heightened the risk of inadvertently, or deliberately, violating the privacy of individuals (Ahmadi et al., 2016). There are also substantial concerns about increased customer data vulnerability and anxiety from such measures in a form of possible data breaches or identity theft (Martin et al., 2017). By alleviating these concerns and allocating resources carefully, a firm can gain a sustainable competitive advantage and maintain healthy customer relationships.

Innovations, such as Internet of Things have made it possible for information to be collected and used to analyse customers very precisely to individually target better advertisement, and to make content and services personalized. IoT could be described as a set of everyday objects with internet connection and/or sensors which people use in their day-to-day activities. Just to name few: smart watch & TV, home security systems and other connected appliances. These devices are being continuously innovated to operate as a part of the network. Hence, it generates huge quantities of data and information and is thus the decisive part of big data.

Analysis of customers' data can be also used to exploit the vulnerabilities of individuals such as advertising free bets for problem gamblers, which intuitionally seems highly unethical. It is showed, that with the big data, it is possible to make accurate predictions of individuals' sensitive information such as sexual orientation, financial status, political/religious views, intelligence and ethnicity even though the data was originally non-identifiable (Kshetri, 2014). This can lead to discrimination and unnecessary

offerings. There are also physical risks associated with the location data, which highlight the importance of sensitive data privacy and security.

The complex and overlapping system of data have created new kinds of vulnerabilities for firms' business secretes or similar sensitive information to be breached, which could negatively affect the firm. Travers, (2023) writes in his news article that hackers are increasingly targeting firm's key individuals to steal credentials on personal devices, which extends the security concerns beyond firm's walls. This new phenomenon of hacking includes, for example, sensitive customer personal data to be held hostage and threatened to leak it publicly to sprawl customer dissatisfaction with the firm's privacy and security measures.

3.1.1 Customers perception of data privacy and security

In the era of big data, secondary use of the customer data has huge potential for more efficient and personalized business models to be innovated. Customers are aware of the potential security threats what the use of personal identifiable data can have, like unauthorized use or misuse, which naturally heightens customers' privacy concerns towards these associated risks. The perception of privacy is rather subjective, and the concerns associated with, for example, authorizing the use of personal data for secondary use is linked with possible privacy outcomes that is resulting from this behaviour. Hence, attitude, intention and behavioural actions form the subjective evaluation that determines customers' willingness to engage in action. Studies have also shown that customers' perceptions of frims' information practices affect customers decision to disclose information with a firm. Findings point highly to customer relationship and trust to the firm's ability to properly handle even sensitive information in intention to action. Consequently, it is shown that third-party audit seals have a weak effect on trust, validating the role of organization's information practices (Libaque-Saenz et al., 2016).

Examining through communications privacy management theory (CPM), customers' intention to disclose personal data forms on the boundary with respect to individuals' disposition to value privacy (DTVP). Customer evaluates to open or not to open the boundary of information flow on few factors. These include cost-benefit ratio, context, motivations, gender and culture as well as the perceived control over the flow of personal information. Evaluation of these factors determines the customer action on possible interaction (Xu et al., 2011). When the boundary is open, the firm becomes co-

owner of the personal information. This creates a certain coordination which includes expectations on how the disclosed information will be used and who has the access. Privacy policies are a coordination mechanism for boundaries which results to firms to be held responsible for proper data management along with the policies, where transparency and control of the data from customer point of view are key areas.

Risk is an uncertainty of negative outcome, and in the context of customer data privacy and security, a possibility of another party's opportunistic behaviour, separate from the customer's true benefits (Xu et al., 2011). This opportunistic behaviour is magnified in the era of big data, as a customer data can be efficiently mined. The effects include, for instance, price-discrimination, exploiting of customer vulnerabilities or reckless utilizing of private data, exposing the customers' data to possible threats. Moreover, number of studies have shown that perceived risk, which in turn raises privacy concerns, do have a negative effect on intentions to conduct transactions in e-commerce (Xu et al., 2011), raising barriers for efficient trade.

3.1.2 Trade-off between value and data disclosure

Libaque-Saenz et al., (2016) describes that previous studies have shown that customers are willing to disclose personal information and allow of the use of user-generated-data (UFD) if there is potential benefits, such as monetary or some non-monetary benefits especially. Libaque-Saenz et al. (2018) reviewed studies have their base on expectancy theory according to which belief that one's extra effort will result in some reward or positive outcome, Advancements in things such as more personalized services have shown to be valued by customers in exchange for personal data.

Services offered B2C have increasingly become free in sense that there is not monetary transaction made, rather the disclosure of user personal data, which allows service providers to utilize it. A cost-benefit trade off can be argued to be present and it includes different calculus made when deciding to do or not to do business with a firm, how desirable is the access, who is the provider and what data management terms they inform.

Mobile phones, which play a key role in IoT in managing different devices of IoT, and the data with it can be thought to represent who we are, as nowadays mobile phones is the device that is always in our pocket. In the case of mobile apps, a user is requested to allow

the developers to have access to the personal information stored in the device in exchange to use of service. Shared information is hence highly personal and can be exposed to fraudulent behaviour. Previous literature of this privacy trade-off has faced criticism, as those argue that the decision to willingness to disclose is rational decision-making process, whereas new forming consensus is pivoting towards the fact of inability of customers to make well informed decisions even though they would have all the information on hand (Wottrich et al., 2018). It is often done almost unconsciously when tapping "allow access". This calls for responsibility from firms to keep the personal data safe as the lack of capability to make informed choices in ever evolving environment is present among customers horded with data gathering points (IoT). It also calls across borders' agreements on definition of privacy and privacy standards to more efficiently interact with other companies and potential customers.

3.2 Challenges with customer data privacy and security

Heightened possibilities for data breach arise from the use and integration of the big data, automatization and other advancements such as AI. With the stream of big data, firms are struggling to integrate sophisticated data bases and analysing methods with data privacy and security in mind, which may undermine the potential benefits of big data (Colombo & Ferrari, 2015). Moreover, the data storing and analysing can be outsourced to a cloud-service provider (CSP), thus creating a larger network for the data and allowing co-control of the data for the service provider. Thus, from a resource-based view, it is vital for firms to allocate their resources accordingly to ensure a competitive edge.

As these challenges are well recognized, it is important to approach these issues with careful examination about is the practices safe and ethical enough? Are the processes and services constructed with customer data privacy and security first? Do we have to collect the data just because we can, and we *may* use it later? Storing of data which does not serve a purpose is a security risk.

Privacy incidents caused by mismanagement of customer data can cause direct economical harm, such as punishments or penalties, loss of market share and failure of customer retention (Gimpel et al., 2018). It is the customer who chooses whether to forgive or not the boundary turbulence which rises from the violating of secure customer data storage. However, firm can and should try to reassure customer.

3.2.1 Firms' measures for data privacy and security concerns

Challenges mentioned on the previous chapter raise the vulnerability of customer data privacy and security. Hence, it is important for the firms to communicate on their data management policies, grant control for the user over his or her data and most importantly be transparent in data management operations. By reducing customers' concerns, we can reduce frictions and barriers in B2C business and innovations regarding to utilizing big data.

There are studies made on specific data privacy measurements which alleviate customers' concerns. Apart from regulations, firms can achieve a competitive advantage from measures that go beyond laws and regulations, thus differentiate themselves from competitors (Gimpel et al., 2018). Examined study was made on interviewing customers in aviation and retail sectors expectations on data privacy and security measures, and to what extent they are expected (Column: factor).

Factor	Customers' expectations	Effect on satisfaction	
		if implemented	if not implemented
Attractive quality (delighter)	Customers do not expect implementation of measure	positive	none
One-dimensional quality (performance need)	Customers explicitly demand implementation of measure	positive	negative
Must-be quality (basic need)	Customers implicitly demand implementation of measure	none	negative
Indifferent quality	Customers are indifferent to implementation of measure	none	none

Study showed that: "In both scenarios, customers can be delighted by storing their data in an anonymized form, empowering them with regard to the combination of their data, and data sharing within the company, and storing their data on servers with a secure location." (Gimpel et al., 2018).

The inherent threat that arises from the use of big data outlines the importance of situational crisis communication theory in the event of unwanted situation. Boundary turbulence forms between customer and firm as a result from violation of the agreement to handle the customer's data securely, especially sensitive data. To maintain a healthy relationship with the customer, with valid retention rate in this inherent environment of possible data breaches, it is vital to build trust and examine the post-crisis communication and respond strategies to help repair reputation and minimize negative consequences for the firm (Chen & Jai, 2021). There can be identified different types of response strategies. Chen & Jai, (2021) identifies as such: "namely, an attack on the accuser, denial, excuse, victimization, justification, ingratiation, corrective action, and full apology strategies". These should be used accordingly to the situational context,

although the author recommends management team to utilize rebuild and full apology strategies in the event of data breach.

Failing to reassure customers and failing to follow a responsible data management policy, has consequences on the firm. Chen & Jai, (2021) points out that violating customers' trust does have a long-term effect on customer loyalty, satisfaction and commitment, which is alarming in the viewpoint of relationship marketing theory as it can diminish the market share of targeted firm. Moreover, it is shown that firms with a low level of transparency versus high level transparency, experience a 1.5 times larger drop in stock price after data breach. Damages from cybersecurity failures and data breaches are estimated to be significant in average of $3.8 million in costs (Martin et al., 2017). This finding arguably creates an incentive to have transparent data management policies as these measures seems to suppress the damaging effects of a data breach.

3.2.2 Firms' responses for customer reassurance

Customer satisfaction can be argued to be in the centre of a successful business. It's constructed of smooth communicational and operational processes throughout the customer journey to maximize the value that can be generated from the business. At present, this process is embedded with the customer data privacy and security at forefront. Hence, it is vital to address the issues and challenges associated with customers perceptions, concerns and expectations regarding to their data. In other words, customer reassurance over their data use.

As briefly discussed previously, among top measures to reassure customers include transparency of firm's data management policies and granting control for customer over their data. Transparency means that the firm is honest about how customers' data will be used by publishing data privacy and management policy. Granting control for customer over their data can be thought of the availability to opt-out from different areas of collection and use of their personal data or from all operations including customer's data collection, analysing and utilizing.

Communicating the purpose of collecting particular data keeps customers and the firm in check on if the data is really needed. As previously mentioned, storing data which does not serve a purpose is a security risk. By informing the purpose and hence the

implementation of customer data for particular purpose reassures the customer to realize the value given in exchange for the disclosed data.

Finally, developing IT and other tools such as AI needs to be built responsibly with sustainable data ethics, to mitigate biases from optimization models and algorithms.

4 Case: Facebook 2018 (Meta)

In 2018 Facebook was accused of allowing the use of its platform's user's data to be misused by a firm called Cambridge Analytica for secondarily analytical purposes without the authorization of those users. Mined data was used to target indifferent voters in U.S presidential election to vote in favour of Donald Trump.

An employee, who worked with Cambridge University academic to mine the data have commented to reporter: "We exploited Facebook to harvest millions of people's profiles. And built models to exploit what we knew about them and target their inner demons. That was the basis the entire company was built on." (Cadwalladr & Graham-Harrison, 2018)

The harvest was made by an application inside Facebook's platform called "thisisyourdigitallife", which was a personality test and users taking the test agreed to have their data collected. However, the app also collected the data of test takers friends, without authorization. (Cadwalladr & Graham-Harrison, 2018)

Facebook had found out about the breach already in late 2015 but did not disclose the information of the breach to the public. This action is opposite from the situational crisis communication theory of recommended practices in such case of boundary turbulence, where violation of agreement of data management terms between firm and customer is apparent: utilize rebuild and full apology strategies. In addition, Facebook did have legal obligation to inform regulators and individuals of the data breach, which is a practice in many states in the U.S. but it choose not to inform the public at the time the misuse was apparent.

Facebook suffered a plunge in its share price, totalling to more than $36 billion in valuation lost in a single day. Also, there was a massive public outrage against Facebook, which undoubtedly undermined the data privacy and security trust in the eyes of its exiting and potential customers.

By examining this particular incident through the lens of this thesis, it is clear that the procedures and measures chosen by Facebook at that time were too little. Facebook were one of the first company to broadly mine its user base and operate in the era of platform-based business models, where regulation were negligible. At present, Facebook have had testimonies and lawsuits about the reckless optimization of its algorithms through UGD. It has caused public dissatisfaction about the polarization effects and other unwanted

externalities that exploitation of user data can potentially sprawl. Facebook is huge and powerful platform, so it is necessary to reconsider its position in society, and hence responsibilities.

5 Discussion and conclusions

After conducting the literature review, we find that there are psychological factors as well as operational factors in the relationship of the phenomena of increase utilization of big data and hence heightened customer data privacy and security concerns. It can be argued that while the network where customers and organizations interact gets more complex, it is the firms' responsibility to handle customers' data with care. As mentioned, customers may not be capable of making informed decisions even though they have all the information on hand. The possibilities that the user generated data allows, outlines the ethical aspect of beneficial use of the data, not just in the sense of firms' economic targets, but also from the overall societal welfare improvement point of view.

The insights that the literature review produced was that there are real concerns of the ethical utilization of big data and the need to alleviate customers' concerns about their personal data use. Consumers are willing to disclose their private information if some offsetting benefits are generated such as more personalized services. Additionally, trust and the relationship between customer and firm seemed to have a strong impact on the level of reassurance needed to engage with the customer. This highlight the need for legislative regulation as well as industries' intra regulation to ensure that these organizations are functioning in customers' benefit. Moreover, the consequences of a data breach do have harmful effects on firms' performance and by being honest and by taking good measurements to prevent it can mitigate the potential harm to the firm.

Firms seem to also lack the skills and systems to utilize big data securely. Therefore, being reckless with the innovations of big data can cause unprecedented harm, weighting the importance of forward-looking big data management strategies with longevity and healthy customer relationships in mind. By acknowledging the best practises, a firm can gain a competitive advantage.

To return to research questions of the thesis, this thesis finds that customers are increasingly worried about their personal data misuse amid big data. It calls for reassuring about the firms' forward looking proper data management policies, with transparency and granted control over the customer data.

Firms have challenges to achieve an absolute secure and privacy measures of their customers' data. Studies have shown that one of the biggest barriers for firms utilizing big data is the uncertainty of secure customer data storage. However, there is pressure for firms to utilize big data as the race for innovations and efficiency improvements is

inherent in business. Therefore, there are risks looming in this field as the customer data privacy and security vulnerabilities rise. By ignoring customers concerns, the negative impacts can be long-lasting and even destructive for the firms doing so. It is vital to have strategies planned for the worst-case scenario.

5.1 Implications to practice

This thesis highlighted concerns among customers about their data use amid big data and examined best practices to interact with customers in the sense of collecting, analysing and using their data in digital era. Data vulnerabilities are something to seriously consider.

Understanding the rapidly evolving business landscape where data privacy and security threats are inherent, firms can gain competitive advantage by doing more than what is required. It shows a responsible and forward-looking strategy which does not try to obscure customers concerns.

Firms should be clear about their data management policies, communicate these practices clearly to customers while also granting control for their personal data while ensuring transparency. These practices reassure customers concerns and build trust.

It is also worth noting that in the case of boundary turbulence, a clear situational crisis communication strategy mitigates the potential damages of violating the boundary agreement of responsible data use and failure to provide the service expected.

5.2 Limitations and future research

This thesis is not a precise look in either on firms' intra operations nor customers' wide demographics. It is rather a literature review on the factors contributing to the challenges regarding to big data's relation to customer concerns about their data use. Moreover, this thesis does not examine the practical implications of data management from legislative framework point of view, but rather a review about the inherent factors affecting this phenomenon.

Implications for future research could focus on legislative framework and what evolvements are happening at that field. There could be also a segmentation of different user demographics regarding their characteristics and how they do perceive the use of their personal data. Moreover, the evolving cybersecurity threats could be investigated thoroughly and by industry to gain insight if there are any unique characteristics and threats evolving.

References

Ahmadi, M., Dileepan, P., & Wheatley, K. K. (2016). A SWOT analysis of big data. *Journal of Education for Business*, *91*(5), 289–294. https://doi.org/10.1080/08832323.2016.1181045

Chen, H. S., & Jai, T. M. (2021). Trust fall: data breach perceptions from loyalty and non-loyalty customers. *Service Industries Journal*, *41*(13–14), 947–963. https://doi.org/10.1080/02642069.2019.1603296

Colombo, P., & Ferrari, E. (2015). Privacy Aware Access Control for Big Data: A Research Roadmap. *Big Data Research*, *2*(4), 145–154. https://doi.org/10.1016/j.bdr.2015.08.001

Gimpel, H., Kleindienst, D., Nüske, N., Rau, D., & Schmied, F. (2018). The upside of data privacy – delighting customers by implementing data privacy measures. *Electronic Markets*, *28*(4), 437–452. https://doi.org/10.1007/s12525-018-0296-3

Hameed, S., Agha, H., & Abbas Choudhary, M. (2012). Shafqat Hameed, Mujtaba Hassan Agha, Muhammad Abbas Choudhary. The Role Of Data Protection Technologies: A Case Study. In *Life Science Journal* (Vol. 9, Issue 4). http://www.lifesciencesite.comhttp://www.lifesciencesite.com.

King, N. J., & Raja, V. T. (2012). Protecting the privacy and security of sensitive customer data in the cloud. *Computer Law and Security Review*, *28*(3), 308–319. https://doi.org/10.1016/j.clsr.2012.03.003

Kshetri, N. (2014). Big datas impact on privacy, security and consumer welfare. *Telecommunications Policy*, *38*(11), 1134–1145. https://doi.org/10.1016/j.telpol.2014.10.002

Libaque-Saenz, C. F., Chang, Y., Kim, J., Park, M. C., & Rho, J. J. (2016). The role of perceived information practices on consumers' intention to authorise secondary use of personal data. *Behaviour and Information Technology*, *35*(5), 339–356. https://doi.org/10.1080/0144929X.2015.1128973

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, *81*(1), 36–58. https://doi.org/10.1509/jm.15.0497

Wottrich, V. M., van Reijmersdal, E. A., & Smit, E. G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems*, *106*, 44–52. https://doi.org/10.1016/j.dss.2017.12.003

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. In *Journal of the Association for Information Systems* (Vol. 12, Issue 12).

Cadwalladr, C., Graham-Harrison, E. (2018) 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach', The Guardian, 17 March.

Travers, K. (2023) 'In a new hacking crime wave, much more personal data is being held hostage', CNBC, 7 May.