Me Too - Value Creation by Digitalization and Data Privacy

Veronica L. Nabbosa
Johannes Kepler University Linz
Institute of Digital Business
Altenbergerstrasse 69, Linz, Austria
+43 732 2468 5544
Veronica.nabbosa@jku.at

ABSTRACT

The paper analyzes two timely business trends: Digitalization and Data Privacy which are deepening their roots globally. Businesses are overwhelmed with enormous quantities of data processed by their internal operations such as website cookies, mobile applications, surveillance cameras, etc. Some even purchase data from data vendors who have better capacity to process it to suit specific business targets. More companies are developing new business models to capture value from the digitalization process. Such business models include Apple Pay, Google Pay, Ali Pay and Lufthansa Miles & More purchase enabled loyalty card which were traditionally companies offering mobile phones, advertising and travel services and core businesses respectively. Other companies are digitalizing partially or wholly their business processes to improve security, these include banks, create convenience by using personal identifying techniques such as fingerprint or facial recognition while others process data and invent business solutions for future use to compete in the market. Previous studies addressed the topics of Business Models without much emphasis on the digital trends and evolving issues such as Data Privacy and Digital Ethics. Comparatively, the topic of Data Privacy has also been argued in biased ways by previous scholars either from a utilitarian point of view where they claimed that privacy should be accorded great importance for businesses only and not individuals or as a basic human right by social scientists and law scholars. We suggest a checklist to minimize risks from both the utilitarian and ethical points of view for enterprises in the digital era.

CCS Concepts

• Security and privacy→Human and societal aspects of security and privacy • Security and privacy→Economics of security and privacy • Information systems→Personalization

Keywords

Data Privacy; Value Creation; Digitalization; Risks; Risk Appetite

ICEBT'20, June 5–7, 2020, Shanghai, China

ACM ISBN 978-1-4503-8778-1/20/06…$15.00
https://doi.org/10.1145/3404649.3404650

1. INTRODUCTION

In 2015, the value of data contributed more than €285 billion (over 1.94% of the EU GDP), only after a year, the value grew to €300 billion representing 1.99% of the GDP. This value is expected to rise to €739 billion (4% of the overall EU GDP) in 2020 if favorable policy and legislative conditions are put in place in time and investments in ICT are encouraged.[12].

Data stimulates new business models and thus stimulates innovation. [2]. More companies are digitalizing business models and processes by utilising data collection methods such as geolocation [11], customization from preferences tracked through social media [1] to generate income, for example through advertising [23], transmitting data to companies which are better equipped to process it [35], etc. examples include Apple Pay, Google Pay, Ali Pay, Miles & More enabled with purchase function (Lufthansa). But others collect for future strategic purposes such as competition for instance, using the data to develop a business solution in case the competitor develops one. The paper will concentrate on evaluating risks against benefits to collect personal data to suggest a checklist when companies may collect data to innovate value creating business solutions.

Unlike selecting a business strategy, designing a business model is more complex as it requires segmenting the market, creating a value proposition for each segment, setting up the framework to deliver that value, and then figuring out various mechanisms to protect business model/strategy from imitation by competitors or disintermediation by customers. [17]. “The essence of a business model is in defining the manner by which the enterprise delivers value to customers, entices customers to pay for value, and converts those payments to profit.”[34].

Moritz Bőhmecke-Schwafert, Crispin Niebel claimed, “indeed, the digital economy and the exponential possibilities it provides not only allows for a multitude of business models in meeting new customer desires but also in creating value for both consumers as well as firms.” [9]. But this is not always the case as many innovations do not turn up into successful business models. Examples of successful technological innovation which failed to get the business model and the technology strategy right included; EMI (the CAT scanner) and Xerox (the personal computer), so did Thomas Edison who had a questionable track record in terms of business model innovation, abandoning the recording business and also failing to get direct (rather than alternating) current adopted as the industry standard for electricity generation and transmission. [29]. The development of the internet has allowed individuals and businesses easy access to vast amounts of data and information, and customer power has increased. [34]. Previous research emphasized data collection for businesses for direct economic purposes such as profitability through advertising, marketing, lock-ins, discriminative pricing, etc. [7], [4]. There are other non-monetary benefits such as Trust and Reputation that companies can thrive on if they collect data ethically to develop business solutions, products, services and processes create [27] and the International Association of Privacy Professionals (IAPP) defines Data Privacy as the right to have some control over how your personal information is collected and used.

[1] **This work received funding from the PERFORM Project which is part of the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 765395.**

2. LITERATURE REVIEW

Early scholars addressed the notion of value creation through the subject of Business Models where they emphasized the 4 major considerations in Business Model formulation being (1) What – Referring to value proposition, (2) who for target customer, (3) How for value network, and why for profit mechanisms. While they mentioned about the 7 IT business trends to watch such as Freemium and social media [15], they did not address issues of data and information which are core in digitalized business models. Paasi Jaakko included the themes of data and information is his paper about business models[27] but still he did not address the issue of related risks. Therefore, this paper will address the gap of risks related to Data and Information within the area of Digitalization to suggest a checklist in order to enhance value created for stakeholders by enterprises.

3. METHODOLOGY

3.1 Search and Selection

To answer the question of how the 2 trends of Digitalization and Data Privacy Compliance generate value to enterprises, a narrative (conventional) [20] literature review covering the following themes was conducted:

1. Innovative Digital Business Solutions
2. Data Privacy in Digitalization
3. Ethical & Economical Risks of Digitalization and Data Privacy.

Table I below summarizes our search and selection which was initiated on Google Scholar after determining the themes which would help in answering the research questions: (1) What would enterprises consider to determine if digitalization (process or business model) would add value to the organization and (3) what would be the best approach to minimize business risk that can potentially be caused by data privacy violations. Articles time range of 10 years (2009-2019) were selected as they intensively covered a depth of knowledge on Digitalization and Data Privacy combined.

Table I: Selection process for literature

Theme	**Innovative Business Solutions** **(1)**	**Data Privacy in Digitalization** **(2)**	**Ethical & Economical Risks of Digitalization and Data Privacy.** **(3)**
Topics Covered	Artificial Intelligence (AI), Big Data, Biometric and Tracking Technologies	Cookies, Web beacons, Profiling, Nonobvious Relationship Awareness (NORA)	Legal risks, 5 Moral dimensions of the Information Age, Key technological trends that raise ethical issues, Risk Analysis Methods
Generated sources/Time in Sec	17,500/13	15,400/0.04	17,80/27
Selected	33	24	7

A total of 64 journal papers and book chapters were handpicked for their relevance to the topic by reading their abstracts, accessibility to full article, publication in English language in our 4 target journals, namely; Information and Computer Security, Electronic Commerce Research, Computer Law and Security Review, and Technological Forecasting and Social Change. To minimize imbalances in our inclusion of source material or objective in viewpoints [8] few papers led to the snowball technique which is a way of finding literature by using a key document on the subject as a starting point. By going through the bibliography in some articles, we found to other relevant titles on the themes above to reinforce our analysis which were not published in our 4 target journals. In addition, recent court cases relating to Digitalization and Data Privacy violations which led to significant economic penalties were analyzed to extract lessons learnt. By applying proven

3.2 Synthesis

Upon conducting a thorough literature review, theme 1 articles (Innovative Business Solutions) had rich findings interconnecting with articles in theme 2 (Data Privacy in Digitalization) but there was insufficient work which discussed theme 3 (Ethical & Economic Risks of Digitalization and Data Privacy) in depth. Basing on the findings from the topics covered in theme 3 (Legal risks, 5 Moral dimensions of the Information Age, Key technological trends that raise ethical issues, Risk Analysis Methods) which we integrated with topics in themes 1 (Artificial Intelligence (AI), Big Data, Biometric and Tracking Technologies) and 2 (Cookies, Web beacons, Profiling, Nonobvious Relationship Awareness (NORA)) to recommend considerations during the digitalization process and compliance to Data Privacy which would lead to value addition for enterprises.

4. INNOVATIVE DIGITAL BUSINESS SOLUTIONS

There are many innovative Digital Business Solutions but we shall focus on 3 major categories determined by their functions which cover most of the enterprises' needs.: Biometric Technologies which are used to ensure maximum security, Tracking Technologies mainly used in Marketing, as well as Assessment Technologies.

4.1 Biometric Technologies

Due to security risks associated with traditional security techniques namely; Firewalls, Anti Malware Software, Intrusion Detection Systems, Internet Protocol Security, Secure Socket Layer and Cryptography, Biometric technology was adopted for highly critical systems. Biometric Technologies can either have physical biometric characteristics such as fingerprints and face recognition or behavioral characteristics such as voice and handwritten signatures. [5].

4.1.1 Face Recognition Technologies

The computer technology which would recognize human faces was invented in 1964 and 1965 by Woody Bledsoe, Helen Chan and Charles Bisson. Since 1997, the technology evolved from 0.54 error rate when it was first tested by the US Department of Defense's Face Recognition Technology to 0.026 in 2006. Facial recognition technology has been adopted by social media websites such as Facebook, it is also currently integrated into consumer software which has posed ethical concerns with data privacy regulators. [3]

4.1.2 Fingerprints

In the late 1990s, 8/10 sales using biometric technology were performed by fingerprint recognition. The technology looks at the friction ridges that cover the fingertips and classify patterns of minutiae, such as branches and end points of the ridges while some have capabilities of looking at the pores in the skin of the ridges. [31]

4.1.3 Handwritten Signatures

These were originally used in China, Korea and Japan as a form of transaction although the upper class people preferred carved personal seals which are still used for serious transactions. Over time, the signature became accepted as the standard way of doing transactions. This can be seen in post offices, banks, and many contracts worth billions of dollars are concluded using this technology. [31].

4.1.4 Voice Recognition

Authentication of a person's voice by this technology is done by storing samples of the voices in a database and matched with the real time voice sample. Background noise should be eliminated to avoid interference with the authentication process due to environmental changes. [31].

4.2 Tracking Technologies - Cookies / IPs

Acquisti and Varian (2005) demonstrate that consumer tracking will raise a merchant's profits only if the tracking is also used to provide consumers with enhanced personalized services. Google is the largest Web tracker, monitoring thousands of websites. Efficiency for online ads is achieved by implementing online technologies which is a combination of cookies and web beacons (Web bugs) which are small programs placed on computers when websites are visited and report back to servers of the beacon owners, the domains and webs visited, ads clicked and other online behavior. [10]

4.3 Artificial Intelligence (AI)

Professors J. McCarthy (Stanford University), M. L. Minsky (Massachusetts Institute of Technology), H. Simon and A. Newell (Carnegie Mellon University) C. E. Shannon (IBM Bell Labs, N. Rochester), and other scholars, first established the concept of "artificial intelligence" at Dartmouth College in the US in 1956. They defined AI as the ability of machines to understand, think, and learn in a similar way to human beings, indicating the possibility of using computers to simulate human intelligence. [28] Since the 1970s, AI has been applied in many business innovations and its development has led to many ethical concerns including Data privacy.

4.4 Big Data

The first definition of Big Data is believed to be the usage of larger volumes of data for visualization by Michael Cox and David Ellsworth. Since then, there are many definitions for Big Data but the commonest one is that from IBM which suggested that Big Data is characterized by 3Vs, namely; Volume (large amounts of data generated from various sources), Variety (using multiple kids of data to analyze a situation) and Velocity (rapid increase of both structured and non-structured data over time causing a need for frequent decision making about the data). Like Artificial Intelligence, Big Data is widely used by enterprises in Decision Making Technologies such as Risk and Credit Assessments. [26]

5. DATA PRIVACY RISKS IN A DIGITALIZED ERA

There is no difference in the definition of risk from both the International Organization for Standardization (ISO) and the Committee of Sponsoring Organizations of the Treadway Commission (COSO) define risk as the possibility that an event will occur that adversely affects the achievement of objectives; risk is described by likelihood and impact by both parties [6].

Digitalization is faced by both opportunities and risks. The risks may include consequences which are directly connect to economic loss such as customer switching leading to reduced revenue, and anti-competition practices such as barriers to entry [32]. Financial Penalties arising from Data Privacy violations and other commercial laws are increasing rapidly. In 2017, Google was fined 2.42 billion Euros for violating the EU antitrust laws [22] and in 2019, French Court issued a fine of €50 million for violating Data Privacy Regulations [13]. Data Privacy Risks are both economic and non-economic to both enterprises and individual customers as discussed below:

- **Dignity**

During the digitalization process, enterprises which do not comply with data privacy practices, do so at the cost of potential compromising of their customers and employees' dignity. While human beings may gain some psychological advantages over disclosing their private data [33] , the problem is all about having control on who discloses this data. The potential risks of having too much information disclosed to the wrong parties may not include only economic disadvantages such as price discrimination but also other forms of discrimination (which may be based on gender, race, income status, etc.), social stigma, embarrassment and blackmailing [4]. Data Privacy has been criticized by early privacy scholars such as Posner as being disadvantageous economically and socially in such a way that it increases the cost of acquiring information and also inhibits innovation as well as business processes such as hiring the right candidates [30], however, other privacy scholars supported it as a fundamental human right which would enable previous offenders for example, to restart a new life and reintegrate positively in society.[25]

- **Good Will**

The increasingly sophisticated scientific devices with capabilities to collect personal information such as geographical location and health related data of body temperature, heartbeat, have created a new sense of urgency in defense of privacy. The concepts of love, friendship and trust which are interconnected to other aspects of humanity such as morality, respect and personality. These are vital aspects which should be protected. [14]. Airbnb, one of the most disruptive digitalized business models faced criticism when it was discovered that a group of Airbnb hosts had been installing secrete surveillance cameras on guests and shared gossip and embarrassing photos of them which challenged the public image of Airbnb. [18]

- **Legal Risks**

Regulators are increasingly playing a more proactive role to protect the privacy of individuals while putting into consideration the business concerns of many enterprises. Some of the popular data privacy regulations include; General Data Protection Regulation (GDPR) which came into force on 25th May, 2019 will be strengthened by the implementation of the e-privacy Regulation soon and the EU-US Privacy Shield which was adopted on 12 July 2016 and became operational on 1 August 2016 to protect the fundamental rights of anyone in the EU whose personal data is transferred to the United States for commercial purposes. It allows the free transfer of data to companies that are certified in the US under the Privacy Shield. Violation of such regulations can potentially cost offenders a huge financial penalty. GDPR violations may be fined up to €20 million, or up to 4% of the annual worldwide turnover of the preceding financial year, whichever is greater.

6. RISK ANALYSIS METHODS

There are two types of risk analysis methods which are widely adopted; (1) Quantitative which use mathematical and statistical tools to measure risk and (2) Qualitative risk analysis methods whereby risk is analyzed basing on interviews instead of mathematics. [19]. The basic formula used to calculate risk is by multiplying the probability of occurrence of security breach by the consequence (impact) of occurrence of security breach [24] which has been extended by other scholars to give more consistent results. Quantitative Risk Analysis has been digitalized into software but sometimes paper based analysis is conducted.

7. RECOMMENDATIONS

Basing on the 5 Moral Dimensions of the Information Age, proposed by Laudon & Laudon, which suggested the following aspects: (1) *Information rights and obligations.* What information rights do individuals and organizations possess with respect to themselves? What can they protect? (2) *Property rights and obligations.* How will traditional intellectual property rights be protected in a digital society in which tracing and accounting for ownership are difficult and ignoring such property rights is so easy? (3) *Accountability and control.* Who can and will be held accountable and liable for the harm done to individual and collective information and property rights? (4) *System quality.* What standards of data and system quality should we demand to protect individual rights and the safety of society? (5) *Quality of life.* What values should be preserved in an information and knowledge-based society? Which institutions should we protect from violation? [10]

Therefore, we propose a checklist which addresses utilitarian and ethical benefits which could enhance value for stakeholders during digitalization:

✓ **Suitability to Risk Appetite**

There several definitions for Risk Appetite but the one from COSO fits this paper the best – "The amount of risk an entity is willing to accept in pursuit of value (it also refers to the degree of risk, on a broad-based level, that a company or other entity is willing to accept in pursuit of its goals)" [6]. Referring to literature from value creation and business models, [16], we integrate the notion of risk in a digitalized business perspective not only in terms of utilitarian and also ethical benefits to help enterprises determine if digitalization is required, or which part of the process can be digitalized or to forego digitalization all the same basing on the assessment from the enterprise's risk appetite.

✓ **Involvement of Stakeholder participation**

Upon analyzing the Technology Acceptance Models which were proposed by Fred Davis in 1989 which emphasized the notions of ease of use and usefulness of the technology, it was suggested that perceived features of a community such as trust be incorporated. [21] As discussed earlier in this paper that it's important for enterprises to maintain good will and respect the dignity of all stakeholders (customers, employees and shareholders) because they all contribute to trust. Loss of trust can directly affect enterprises with both utilitarian benefits such as loss of revenue and also ethical negative consequences.

✓ **Compliance to Regulations**

Digitalization should not compromise regulatory aspects such as commercial laws of anti-trust, competition, consumer protection, as well as Data Privacy Compliance, among others to address ethical and legal dilemmas which are increasingly becoming costly. As earlier mentioned in this paper, In 2017, Google was fined 2.42 billion Euros for violating the EU antitrust laws [22] and in 2019, French Court issued a fine of €50 million for violating Data Privacy Regulations [13]. Other examples include Facebook which was fined US$5 billion and British Airways, 183 British Pounds for Data Privacy related violations.

8. CONCLUSION

While it is impossible to calculate the negative utility coming from future potential misuse of personal information, [1] it can be minimized. We were not able to propose a digitalized business model which integrated topics of value creation to risks, data privacy and digital information with pressing ethical concerns in today's business environment but we are hopeful that future research will address this research gap. Therefore, it's necessary for enterprises to first assess the risks involved by using either qualitative or quantitative methods, keeping in mind ethical concerns especially relating to data privacy to make an informed decision whether partial and whole digitalization is necessary.

9. ACKNOWLEDGMENTS

Our thanks to Prof. Stefan Koch, Vice- Rector of Academic Affairs at Johannes Kepler University, Linz, Austria who reviewed the paper internally to guide us to vital sources which improved our work.

10. REFERENCES

[1] Acquisti, A. (2001). Privacy and Security of Personal Information: Technological Solutions and Economic Incentives. Economics of Information Security, (April 2006), 1–25. https://doi.org/10.1007/1-4020-8090-5

[2] Acquisti, A., Gross, R., & Stutzman, F. (2014). Face Recognition and Privacy in the Age of Augmented Reality. Journal of Privacy and Confidentiality, 6(2), 1–20. https://doi.org/10.29012/jpc.v6i2.638

[3] Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. Journal of Economic Literature, 54(2), 442–492. https://doi.org/10.1257/jel.54.2.442

[4] Arshad, M. J., Iqbal, A., Farooq, A., Khan, M. U. G., Afzal, M., Wajid, A., & Nasir, A. (2014). A Study of Internet Threats, Avoidance and Biometric Security Techniques - Comparison of Biometric Techniques. Journal of Faculty of Engineering & Technology (JFET), 21(2), 135–146.

[5] Belleflamme, P., & Vergote, W. (2016). Monopoly price discrimination and privacy: The hidden cost of hiding.

Economics Letters, 149, 141–144. https://doi.org/10.1016/j.econlet.2016.10.027

[6] Böhmecke-Schwafert, M., & Niebel, C. (2019). the General Data Protection'S (Gdpr) Impact on Data-Driven Business Models: The Case of the Right to Data Portability and Facebook, (January). Retrieved from https://www.itu.int/en/journal/002/Pages/default.aspx

[7] European Commission Data Policy and Innovation (Unit G.1). (2019). Building a European data economy. Retrieved from https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy

[8] Fried, C. (1968). Privacy. Yale Law Journal, 77(3), 9–14. https://doi.org/10.1007/978-1-4302-3543-9_2

[9] Harreid, J. B., O'Reilly, C. A., & Tushman, M. L. (2007). Dynamic capabilities at IBM: Driving strategy into action. California Management Review, 49(4), 21–43. https://doi.org/10.2307/41166404

[10] Holmes, A. (2019). Is your Airbnb host spying on you with a hidden camera? Use this simple trick to find out. The Business Insider. Retrieved from https://www.businessinsider.de/airbnb-host-spying-hidden-camera-how-to-find-trick-2019-11?r=US&IR=T

[11] Karabacak, B., & Sogukpinar, I. (2005). ISRAM: Information security risk analysis method. Computers and Security, 24(2), 147–159. https://doi.org/10.1016/j.cose.2004.07.004

[12] Laudon, K. C., & Laudon, J. P. (2003). Management Information Systems: Managing the Digital Firm. (E. Svendsen, S. Yagan, & B. Horan, Eds.), Revista de Administração Contemporânea (TWELFTH ED, Vol. 7). Pearson Prentice Hall. https://doi.org/10.1590/s1415-65552003000100014

[13] McEvoy, N., & Whitcombe, A. (2002). Structured Risk Analysis.

[14] Noam, E. M. (1995). Privacy in Telecommunications: Markets, Rights, and Regulations. Part III: Markets in Privacy. New Telecom Quarterly, (4), 51–60.

[15] O'Leary, D. E. (2013). Artificial intelligence and big data. IEEE Intelligent Systems, 28(2), 96–99. https://doi.org/10.1109/MIS.2013.39

[16] Pan, Y. (2016). Heading toward Artificial Intelligence 2.0. Engineering, 2(4), 409–413. https://doi.org/10.1016/J.ENG.2016.04.018

[17] Pisano, G. P., & Teece, D. J. (2007). Management.

[18] Posner, R. A. (1977). The Right of Privacy GEORGIA LAW REVIEW THE RIGHT OF PRIVACY, 393. Retrieved from http://chicagounbound.uchicago.edu/journal_articles

[19] Sandhu, P. S., Kaur, I., Verma, A., Jindal, S., & Singh, S. (2009). Biometric Methods and Implementation of Algorithms. World Academy of Science, Engineering and Technology International Journal of Computer and Information Engineering, 3(4), 1033–1038.

[20] Tamir, D. I., & Mitchell, J. P. (2012). Disclosing information about the self is intrinsically rewarding. Proceedings of the National Academy of Sciences of the United States of America, 109(21), 8038–8043. https://doi.org/10.1073/pnas.1202129109

[21] Teece, D. J. (2010). Business models, business strategy and innovation. Long Range Planning, 43(2–3), 172–194. https://doi.org/10.1016/j.lrp.2009.07.003