Societal and Ethical Issues of Digitalization

Veronica Nabbosa
Johannes Kepler University Linz
Altenbergerstrasse 69
Linz 4040, Austria
Veronica.nabbosa@jku.at

Claudia Kaar
Johannes Kepler University Linz
Altenbergerstrasse 69
Linz 4040, Austria
Claudia.Kaar@jku.at

ABSTRACT
The paper intends to analyze two timely trends: Digitalization and associated Digital Ethics, both of which are deepening their roots globally. Data is thought to be the cornerstone of these trends: where once firms were overwhelmed by large quantities of unused structured and unstructured data, they are increasingly adapting their operations and value creation models, guided both by new digital tools and the data themselves. Website cookies, mobile applications, and surveillance cameras, as well as data from third-party vendors, have thus become the new “digital oil”, as firms exploit process and customer data in pursuit of digitalization. Established firms’ core business models have shifted in response to data availability: Apple Pay and Google Pay (operating systems), AliPay (e-commerce), and Lufthansa’s Miles & More purchase enabled loyalty card (travel) emerged from old, established businesses. Still, other firms are partially or wholly digitizing existing business processes in order to respond to the challenges posed by digitalization. Banks, for instance, are using fingerprint and facial recognition to make their services more convenient and to improve security. These developments are not only visible among competitive private sector firms: the public sector is also becoming digitalized, not only to promote efficiency but also to promote transparency and accountability. However, customers and citizens are waking up to the fact that their information is being collected by both private and public entities, and have begun to demand control and transparency. Governments and other regulating bodies (ISO, ACM, and IEEE, among others) are taking a more proactive role in responding to these demands. This paper will delve into the tensions inherent in digitalization, zooming in on digital ethics, shifts in societal values, utilitarian benefits and risks, the future of digitalization, the role of technology in digital ethics, and other themes which could impact all society stakeholders and raises question about ethical issues in several topics.

CCS Concepts
•Security and privacy→Software and application security→Social network security and privacy •Security and privacy→Software and application security→Social network security and privacy

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.

ICBDM 2020, May 15–17, 2020, Manchester, United Kingdom
© 2020 Copyright is held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 978-1-4503-7506-1/20/05...
$15.00
https://doi.org/10.1145/3437075.3437093

Keywords
Digitalization; Digital Ethics; Social and Ethical Issues

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 Information and Communication Technologies (ICT) are encouraged. (European Commission, 2019).

Data stimulates new business models and thus stimulates innovation (Acquisti, 2014). More companies are digitizing business models and processes by utilizing data collection methods such as geolocation (Kosinski, Stillwell, & Graepel, 2013), customization from preferences tracked through social media (Acquisti, 2004) to generate income, for example through advertising, transmitting data to companies which are better equipped to process it, 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 development of the internet has allowed individuals and businesses easy access to vast amounts of data and information, and customer power has increased. Previous research emphasized data collection for businesses for direct economic purposes such as profitability through advertising, marketing, lock-ins, discriminative pricing, etc. (Acquisti, Taylor, & Wagman, 2016; Belleflamme & Vergote, 2016). 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.

Digitalization is the interconnection of the technology, the business model, the data and information that the digital technology in the products, services, and processes create (Paasi, 2017). Data Privacy is defined as the right to have some control over how your personal information is collected and used by the International Association of Privacy Professionals (IAPP).

However, before going into detail about the societal and ethical issues of digitization, we need to understand what digital ethics are. Rafael Capurro coined the definition of digital ethics. He describes it as follows: “I define “digital ethics” or “information ethics” in a narrower sense as dealing with the impact of digital ICT on society and the environment at large as well as with ethical questions dealing with the Internet digital information and communication media (“digital media ethics”) in particular.” (Capurro, 2009).
The purpose of this paper is to describe the societal and ethical issues of digitalization. Today’s literature shows six different themes in which social and ethics issues are of concern by digitalization, privacy, autonomy, safety and security, balance of power, human dignity, and justice (Royakkers, Timmer, Kool, & van Est, 2018).

This paper is structured as follows: In Section 2 a brief theoretical background from other scholars on the issues of digitalization and ethics. Section 3 will describe innovative digital solutions stemming from the information society. The utilitarian and hedonic benefits of digitalization will be shown in Section 4, whereas Section 5 depicts societal and ethical concerns of digitalization. Section 6 will conclude this paper.

2. DIGITALIZATION & GLOBAL PLAYERS

Digitization and digitalization, especially involving data, stimulate new business models and thus stimulate innovation (Acquisti, Gross, & Stutzman, 2014). Many firms are digitizing business models and processes by utilizing data collection methods such as geolocation (Kosinski et al., 2013), customization from preferences tracked through social media (Acquisti, 2004) to generate income, for example through advertising, transmitting data to companies which are better equipped to process it (Shapiro & Varian, 1997). However, this use of data and digital tools has both micro and macro-level implications and is being driven by digitalization by both private firms and public actors. On the micro-level, individuals are increasingly concerned about how their data is collected, used and stored (Bogusz, 2019), and this has driven grassroots movements, new privacy-protecting services, and the development of new regulations. Data and digital tools have also changed and shaped individual behaviors: from children addicted to computer games (Coeckelbergh, 2007), to changing their online and offline behaviors in response to surveillance technologies (Nagenborg, 2014). On the macro level, digitalization has implications for equality, the environment, and society more broadly. For instance, the Digital Economy is consistently dominated by the USA, China and the EU in a distant 3rd position. The USA and China account for 75% of all patents related to blockchain technologies, 50% of global spending on IoT, and more than 75 percent of the world market for public cloud computing. And the two countries also account for 90% of the market capitalization value of the world’s 70 largest digital platforms. Europe’s share is 4% and Africa and Latin America’s together is only 1%. Seven “super platforms” – Microsoft, followed by Apple, Amazon, Google, Facebook, Tencent, and Alibaba – account for two-thirds of the total market value (United Nations, 2019). However, these different countries and regions have different rules around the treatment of data, surveillance, and the environment-likely to affect how digitalization occurs and its implications for society in the future.

3. INNOVATIVE DIGITAL SOLUTIONS

There are many innovative digital business solutions but we shall focus on three 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.

3.1 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 (Junaid Arshad et al., 2014).

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 (Acquisti et al., 2014).

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 endpoints of the ridges while some have capabilities of looking at the pores in the skin of the ridges (Sandhu, Kaur, Verma, Jindal, & Singh, 2009).

Handwritten Signatures

Handwritten signatures 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 (Sandhu et al., 2009).

Voice Recognition

Authentication of a person’s voice by this technology is done by storing samples of the voice 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 (Sandhu et al., 2009).

3.2 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 tracking technologies which are a combination of cookies and web beacons (Web bugs) which are small programs placed on computers when

---

1. This work has received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie PERFORM project, grant agreement No. 765395
websites are visited and report back to servers of the beacon owners, the domains and webs visited, ads clicked and other online behavior (Laudon & Laudon, 2017). Comparatively, An Internet Protocol protocol address (IP address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IP address serves two main functions: host or network interface identification and location addressing.

3.3 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 (Pan, 2016). Since the 1970s, AI has been applied in many business innovations and its development has led to many ethical concerns including data privacy.

3.4 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 most common one is that from IBM. They suggested that big data is characterized by 3V’s, 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 AI, big data is widely used by enterprises in decision-making technologies such as risk and credit assessments (O’Leary, 2013).

4. UTILITARIAN AND HEDONIC BENEFITS OF DIGITIZATION
Digitalization is faced by both opportunities and risks. The risks may include consequences which are directly connected to economic loss such as customer switching leading to reduced revenue, and anti-competition practices such as barriers to entry (de Reuver, Sørensen, & Basole, 2018). Financial penalties arising from standard violations and other commercial laws are increasing rapidly. In 2017, Google was fined 2.42 billion Euros for violating the EU antitrust laws (Lin, 2016) and in 2019, French Court issued a fine of €50 million for violating Data Privacy Regulations (van der Wolk et al., 2019). We discuss the benefits of digitalization from two points of view. The utilitarian, or also economics view, and hedonic view, which will focus on ethics and society.

4.1 Dignity
This is a component of the ethical aspect of Data Privacy and Security. Innovative digital solutions have made it possible to process data quickly and securely. There are many globally accepted regulations, standards, and policies but we shall discuss only four below:

Health Insurance Portability and Accountability Act (HIPAA)
HIPAA was enacted in 1996 in USA to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.

Payment Card Industry Data Security Standards (PCI-DSS)
PCI-DSS is a set of security standards developed by major credit card companies to help protect sensitive cardholder data. Its compliance requirements are contractual commitments, not government regulations, maintained and enforced by the Payment Card Industry Security Standards Council (PCI SSC), an independent global body established in 2006. PCI-DSS applies to all merchants or organizations that accept, transmit, or store cardholder data. However, there are different PCI-DSS compliance levels depending on the number of payment transactions that a merchant/organization has handled over the previous twelve months.

The Protection of Personal Information Act (POPI)
POPI was enacted as a law in South Africa in 2014. Its key objective is to protect personal information collected in the public and private spheres. Under POPI, South African institutions must adhere to a set of compliance standards that ensure responsible collecting, storing, processing, and sharing of personal information. POPI applies to all South African companies, though it is aimed specifically at entities that handle vast amounts of consumer information such as banks, medical organizations, and insurance companies. The law not only protects individuals but extends to any legally recognized entity, including companies and communities. Under POPI, consumers have access to their data, can request its deletion or modification, and control with whom it is shared. Companies are required to collect data for valid and transparent reasons, retaining it only as long as it is strictly needed. Moreover, they must adhere to security compliance standards; ensuring data is not breached or compromised, on their part or on the part of any third parties that may process the data on their behalf. Failing to meet POPI requirements can lead to reputational damage, fines, and imprisonment.

General Data Protection Regulation (GDPR)
GDPR was enacted in 2018 to facilitate the free flow of personal data within the European Union and to protect the privacy of residents within the Union. GDPR is comprehensive and has been praised to be the “gold standard” by some practitioners. The former supervisor of the European Data Protection Board, the late Giovanni Buttarelli (May his soul rest in peace) described the regulation as being robust and flexible to foster trust and accountability, by being transparent and accessible to stakeholders as well as being efficient in providing relevant and timely guidance on compliance, a game-changer which embraces accountability as a cornerstone for ethical responsibility in conducting activities which take place for a given purpose, whether profit-making, law enforcement, social care or research – or even a combination of them and a data privacy bridge which can stand the test of time.

Without digitalization, formulating, implementing and scaling of such regulations, policies, and standards would be a nightmare. During the digitization process, enterprises which do not comply with data privacy practices, do so at the cost, potentially compromising their customers' and employees’ dignity. While human beings may gain some psychological advantages over disclosing their private data (Tamir & Mitchell, 2012), the problem is all about having control over 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 (Acquisti et al., 2016). Data privacy has been criticized by early privacy scholars such as Posner (1977) 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. 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 (Noam, 1995).

4.2 Goodwill
Digital policies, standards, and regulations make it easier for both private and public entities to build goodwill through governance, compliance, and transparency. The increasingly sophisticated scientific devices with capabilities to collect personal information such as geographical location and health-related data of body temperature or 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 (Fried, 1968). Airbnb, one of the most disruptive digitized business models faced criticism when it was discovered that a group of Airbnb hosts had been installing secret surveillance cameras on guests and shared gossip and embarrassing photos of them which challenged the public image of Airbnb (Holmes, 2019). Through digital social networks, it was possible to expose this undesirable practice by Airbnb hence attracting a fast response to resolve the issue.

4.3 Efficiency and Transparency in Service Delivery
In both private and public sectors, we have witnessed increased levels of efficiency and transparency. The development of online systems to apply for loans in financial institutions, online visa applications, are some of the digital benefits which promote transparency and efficiency. The India Stack which is a set of Application Program Interfaces (APIs) that allows governments, businesses, startups, and developers to utilize a unique digital Infrastructure to solve India’s hard problems towards presence-less, paperless, and cashless service delivery. The Digital Locker eliminates physical paper and fake documents by issuing documents digitally, while the eSign service allows all national ID holders to digitally sign documents and request digital signatures.

4.4 Enhanced Economic Benefits
Richard A. Posner, an American Judge, in his article, The Economics of Privacy, while arguing against privacy to data to be emphasized on individuals, he acknowledges that sharing and processing such data by digital means saves the cost of business processes such as hiring a person with a serious criminal record unknowingly and later end up in a lengthy court process which costs a lot of money and time. Other economic benefits of digitalization include but are not limited to enhanced profitability through price discrimination for online customers which is possible through tracking cookies which monitor their shopping behavior. Other techniques such as upselling and cross-selling are also possible through digitalization. These also enhance the profitability of enterprises.

5. SOCIAL AND ETHICAL CONCERNS OF DIGITALIZATION
Through new technologies, innovative digital solutions are established. Companies and governments can benefit from the new ways of treating data. However, not every major breakthrough in technology is reviewed about their moral and ethical implications. Based on a literature review conducted by Royakkers et al. (2018),

1 https://www.brookings.edu/blog/techtank/2018/08/23/indias-data-dilemma-how-to-protect-all-of-it/

several themes were found which appeared though digitalization and effect social and ethical issues, namely privacy, autonomy, safety and security, balance of power, human dignity and justice. The following section will go into detail of the different themes and raise questions about the ethical and social concerns.

5.1 Privacy
Smart devices like the amazon dot, smart fridges, lamps, etc. collect data around the clock. Even though the manuals and the general terms and conditions state that data is collected and transmitted to third parties, we, however, give permission. We suffer from consent fatigue, which is an overload of information on terms and conditions we are not able to sort through anymore. The collected data provides information about our whereabouts, likes and dislikes, and even more private and personal information. The collected data belongs to the manufacturer and endangers the privacy of our own personal data. In the healthcare sector, more and more gadgets and tools are used to monitor patients. The collected data concerns exceedingly sensitive and private data.

With the help of biometric technology, privacy can on the one hand and be used to protect it, and on the other hand, be exploited. An example where privacy with biometric technology can be ensured is the use of e-gates at airports. Nowadays the passport is scanned and a picture is taken of your face. Through face recognition software, the picture is compared with the one stored in the passport and a decision about the rightful owner is made. Hereby, no data is exploited because it just compared with the stored image. On the other hand, biometric data like about a person's health can be used against him or her, e.g., by insurance companies. New trends to detect emotions and a person's current mood show that people's mental privacy is in danger.

Augmented Reality has also an impact on privacy. For example, with the Google Glass, everybody who wore the glasses took a video of wherever they went. Here people that did not want to be filmed or analyzed were captured without their consent. Due to the huge backlashes of the public about privacy concerns, Google stopped the production of the glasses in 2015.

An issue often overlooked is the power of platform providers. Next to Facebook and Twitter, Uber and others are able to track every movement of a person on the platform. They know their ratings, likes and dislikes, and are able to predict certain preferences. Here the data also leads to penetration of our privacy.

Ethical issues in the area of privacy arise, for example, Who’s is the owner of the data? Does the manufacturer have any responsibilities? Should there be any regulations in data collection? These are just some issues which currently concern governments and regulators. Through data protection laws, regulators try to shift the data rights back to the user and not the manufacturer.

5.2 Autonomy
The be autonomous means to be “independent and having the power to make your own decisions”. The autonomy of people is widely affected by the ongoing trend of digitalization. A recurring theme in autonomy is the concern, that IoT systems know better than we do. This paternalism of technology means that the technology makes the decision for us. IoT systems are able to decide, e.g., what should be ordered by the fridge if it detects too much calories.
Nowadays, technology is able to control and manipulate the users’ behavior and reduce their autonomy. However, persuasive technology could train users to display the desired norm. For example, if you do not put your seatbelt on, the car starts beeping and only stops if the person fastens their seatbelt. This persuasion of technology actually helps to reduce major injuries in car crashes, but also raises the question if we are manipulated and stimulated through technology in other areas. The persons’ autonomy can be restricted if persuasive technology controls our behavior without our active knowledge.

Smart devices and even social media are able to steer our preferences. By showing us only “relevant” information, people are steered in a desired direction. A prominent example of steering people’s preferences are the presidential elections in the United States in 2016 (The Guardian, 2020). By using big data analyses and personalized content the company Cambridge Analytica was able to shift voters’ positions. By showing undecided voters bad content about the opposing party, voters could be manipulated into voting for the other party.

Through the uprising of artificial intelligence and robotics, more and more autonomous vehicles and devices are produced. Through their high computing power and algorithms, robots are able to make a decision within nanoseconds. In the military, unmanned drones are used to surveil or even attack enemy territory. By detaching the actual human from the machine, decisions about life and death are apparent. Also with self-driving cars, the question arises, who makes the decision, about either crashing the car and let the driver die or crashing into a child and the driver survives. Scholars agree that only humans can make life and death decisions, and the robot should never be able to make such moral decisions. Ethical questions arise like to what extent are people controlled and manipulated? Is it the job of the technology to train our behavior? Who decides what the norms are? Should robots decide on life and death? Can a robot be responsible for killing someone?

5.3 Security
Through the penetration of IoT in our everyday lives, security plays a crucial role. However, attacks on systems through hackers happened constantly. In early January of 2020, the Federal Ministry of Foreign Affairs of Austria is under a DDoS (Distributed Denial of Service) attack (Kurier, 2020). Which restrain the use of IT systems and websites? Until now the Ministry is still not sure if data was tapped. With smart devices in our homes, hackers are able to penetrate does systems, and are able to manipulate and even threaten human lives, i.e., with medical devices. Moreover, biometric system can also be hacked. By intentionally obtaining someone’s identity, hackers are able to, e.g., copy the fingerprint of the German Minister of Defense, which was shown at the Chaos Communication Congress in 2014 (Hern, 2014).

Another issue is safety in the virtual world. With VR technologies, people are able to almost fully commit to a virtual world. By exploiting these worlds and, e.g., creating avatars which assault people. Psychological damage can occur through the emotional involvement of the user. However, virtual meetings will be the future and questions about the safety and wellbeing of the user need to be considered. Society faces ethical dilemmas in the area of security and safety. But questions like How can we protect us from stolen data? Or how do we keep our lives private and “disconnected” from the virtual world? are just some which need to be answered.

5.4 Balance of Power
People are experiencing a lock-in effect if it comes to smart devices and the corresponding software. The delivered hardware comes with software and is maintained by the manufacturer. We often only can use the hardware if we use the software. Manufacturers are the ones to decide what services we are able to use or not. A big problem in this fast-evolving area is the dropout or takeover of certain manufacturers, which means that services often are not carried forward.

Other issues concerning the balance of power are unfair conditions or monopolization. As in the example before, Tech companies are often taken over by even bigger firms and shifting to a monopoly. With platforms like Airbnb, hosts are not following the actual rules for hotels and are able to not pay taxes on their rented rooms. Network effects often happen, because platforms are dependent on their users.

Moreover, the data collected from our posts, likes and dislikes, is stored with the platform owner. They are able to decide what to do with the data and even sell it. Bigger issues appear if the government starts to collect data on own us and starts using it against us. A prominent example is the Chinese government that keeps a citizen score of every person and determines, e.g., what kind of credit score they get or how high are their insurance fees.

Questions raised in this area are Who sets the standards and is responsible that we follow them? Are platforms or governments allowed to use data against a person? Do platform providers have to follow the set of rules implemented by the government? Balance of power is something to not underestimate as it shifts our view to the ones of the operator.

5.5 Human Dignity
Through the uprising of robots questions on dehumanization arise. If we implement robots for caretaking tasks, we risk losing the sense of human interaction. It is argued that robots should only handle tasks that do not need emotional and personal involvement, as it is shown that empathy and human contact are pillars of good care. Therefore, if robots start taking care of people, we risk of people feeling objectified and dehumanized.

Recently discussed in media and governments is the overtake of robots in the industry. People fear of losing their jobs to robots and are not able to find new work. Two sides to this issue occur. One the one side, the use of automation and robots bring economic growth and the workforce’s education shifts to not doing the task but handling the robot. On the other hand, fewer jobs are offered and therefore prosperity is declining.

Biometric systems are in danger of being instrumentalized. By defining an ideal or standard user in the system, people who do not comply with the norm are flagged or treated differently. For a motorist in the United States, a mistake in the system flagged him and got his license taken away, even though he did not do anything wrong. It took several days to correct the mistake and to get his license reinstated.

As mentioned before, persuasive technology is able to guide us to a safer environment, like the seatbelt example. However, if we are constantly in need of persuading tools, we often lose sense of what is right and wrong. We start to depend on the technology to tell us if we drive to fast, or are too close to the vehicle before us. This could lead to a behavior change in the human itself.

With VR technologies, people are able to almost fully commit to a virtual world and lose the sense of their own bodies. This often
leads to people losing touch with the real world and their own bodies. This issue will be even bigger in the near future, as technology in the area of VR evolves quickly.

Ethical issues in these areas arise because of robotics and new technologies. People fear losing touch or get replaced by robots. Dehumanization often appears by involving robots and technologies in tasks and raises questions on how to deal with the shifting attitudes toward technology.

5.6 Justice
As mentioned before, biometric systems are able to categorize people into certain groups, like criminals or terrorists. The stigmatization of people and their perceived identity in the system is often hard to prove differently.

Platform owners are enabled to restrict the use of certain users. They can exploit the regulations and, e.g., be able to let people work for under the minimum wage or restrict their use because of low ratings. Cases show that female job seekers do not get offered the same positions as male job seekers with the same qualification, because of applied algorithms. Justice in the area for new technology becomes apparent. But questions like Who implements the rules? and How we can overcome stigmatization? are still unsolved.

The themes show a general direction on what areas of our lives are at risk of losing morals standards by the implementation of new technologies. Scholars, regulators, and governments all over the world try to tackle raised ethical questions. With data protection laws we did the first step to shift the ownership of our data back to the user. However, in newer areas like biometric systems, we still face ethical questions and how it should be used and by whom.

Amidst increasing popularity of new technologies and the awareness of users about data, ethical issues are a crucial topic in today's society. Through digitalization, new business models and strategies are in development. Companies like Facebook, Uber, Amazon, etc. profit from the huge amount of data that is generated by us users. Even governments and regulators use new technologies like biometric systems to change the way we used to tackle problems. IoT and smart devices already found a way into our homes.

These new technologies enable us to work “smarter” and in new ways. The questions however are, at what costs? The generated data can, on the one hand, be used to help us and make our lives easier, but on the other hand, can also be exploited. Ethical issues in the way our data is treated arise. Since couple of years’ scholars, governments, companies, and society discuss moral issues arising from new technologies. We presented six main themes which are currently in discussion: privacy, autonomy, safety and security, balance of power, human dignity, and justice.

In the area of privacy, we raised questions about who the owner of the data is and if manufacturers have any responsibilities. Even though, data protection laws force companies to be more responsible with our data, we still have many issues to discuss. Autonomy is an area we should not overlook. New technologies are able to control and even manipulate our behavior. Positive persuasive technology can save lives, but also threaten our awareness in the context of manipulation and social norms. Whereas security and safety are topics who are widely discussed since the 70s. Often only the technical part is considered. Question about how do we keep our life disconnected to the virtual world is only one questions arising from the use of new technologies. New business models and technology also raise the question of power.

Software and hardware packages lead to lock-in and network effects across the globe. Employment and industrial laws are bypassed through unclear regulations. Ethical issues about rule implementation and enforcement are still not answered. The fear of robots taking away our jobs is related to the issue of human dignity. Robots are capable of doing almost every task now but do we want robots to overtake everything. Should we allow robots to make life and death decisions, or is a human component crucial to not lose touch to the real world? How justice can be enforced in the shown themes is only the tip of the iceberg, and needs thorough consideration in the context of new technologies.

6. CONCLUSION
While we cannot give any answer to the raised ethical questions, interdisciplinary scholars from social science, technology, law and business need to pay attention to the growing concern of ethical and data privacy issues amidst the dynamic technological trends in Digitalization both within private and public sector. The awareness and sensitivity to data privacy needs to be strengthened. Services about data protection need to be enforced and the property of the data needs to shift back to the user whereas companies need to comply with the stricter rules. Regulation alone cannot achieve everything, hence a call to ethical accountability by all stakeholders.

7. ACKNOWLEDGEMENTS
This work would not be possible without the generous funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie PERFORM project, grant agreement No. 765395

8. REFERENCES
[1] Acquisti, A. (2004). Privacy and Security of Personal Information. In Economics of Information Security (pp. 179–186). https://doi.org/10.1007/1-4020-8090-5_14

[2] Acquisti, A. (2014). The Economics and Behavioral Economics of Privacy. In Privacy, Big Data, and the Public Good: Frameworks for Engagement (pp. 76–95).

[3] Acquisti, A., Gross, R., & Stutzman, F. D. (2014). Face Recognition and Privacy in the Age of Augmented Reality. Journal of Privacy and Confidentiality, 6(2), 20.

[4] 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

[5] Acquisti, A., & Varian, H. (2005). Conditioning Prices on Purchase History. Journal of Marketing Science, 24(3).

[6] 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

[7] Bogusz, C. I. (2019). Digital identity – beyond verification. In Digital Transformation and Public Services (pp. 214–232). https://doi.org/10.4324/9780429319297

[8] Capurro, R. (2009). Digital ethics. Global Forum Civilization and Peace, 207–2016. The Academy of Korean Studies. UNESCO.

[9] Coeckelbergh, M. (2007). Violent computer games, empathy, and cosmopolitanism. Ethics and Information Technology, 9(3), 219–231. https://doi.org/10.1007/s10676-007-9145-3

[10] de Reuver, M., Sørensen, C., & Basole, R. C. (2018). The Digital Platform: A Research Agenda. Journal of
Information Technology, 33(2), 124–135. https://doi.org/10.1057/s41265-016-0033-3

[11] European Commission. (2019). Data Policy and Innovation (Unit G.1).

[12] Hern, A. (2014). Hacker fakes German minister’s fingerprints using photos of her hands. Retrieved January 7, 2020, from https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands

[13] Junaid Arshad, M., Iqbal, A., Farooq, A., Ghani Khan, M. U., Afzal, M., Wajid, A., & Nasir, A. (2014). A Study of Internet Threats, Avoidance and Biometric Security Techniques - Comparison of Biometric Techniques. Implementation Science, 21(2), 135–146. https://doi.org/10.4324/9781315853178

[14] Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. Proceedings of the National Academy of Sciences of the United States of America, 110(15), 5802–5805. https://doi.org/10.1073/pnas.1218772110

[15] Kurier. (2020). Cyberangriff auf Außenministerium läuft noch immer. Retrieved January 7, 2020, from https://kurier.at/politik/inland/cyberangriff-auf-aussenministerium-lauft-noch-immer/400718463

[16] Laudon, K. C., & Laudon, J. P. (2017). Management information systems: managing the digital firm (Fifteenth). Harlow London NY: Pearson Education Limited.

[17] Lin, R. (2016). Sole Structure Design for the Disabled. International Journal of Advanced Engineering and Management Research, 1(2), 94–100.

[18] Nagenborg, M. (2014). Surveillance and persuasion. Ethics and Information Technology, 16(1), 43–49. https://doi.org/10.1007/s10676-014-9339-4

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

[20] O’Leary, D. E. (2013). Artificial Intelligence and Big Data. IEEE Intelligent Systems, 28(2), 66–99.

[21] Paasi, J. (2017). Business models in the future of manufacturing. In Towards a new era in manufacturing, Final report of VTT’s For Industry spearhead programme (pp. 24–33). VTT Technical Research Centre of Finland.

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

[23] Posner, R. A. (1977). The Right of Privacy. Georgia Law Review, 393. Retrieved from http://chicagounbound.uchicago.edu/journal_articles

[24] Royakkers, L., Timmer, J., Kool, L., & van Est, R. (2018). Societal and ethical issues of digitization. Ethics and Information Technology, 20(2), 127–142. https://doi.org/10.1007/s10676-018-9452-x

[25] 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.

[26] Shapiro, C., & Varian, H. R. (1997). US Government Information Policy.

[27] 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

[28] The Guardian. (2020). The Cambridge Analytica Files. Retrieved January 7, 2020, from https://www.theguardian.com/news/series/cambridge-analytica-files

[29] van der Wolk, A., Tigner, R., & Famigletti, R. N. (2019, January). C’est It Ain’t So: French DPA Issues Google Largest GDPR Fine to Date. Morrison & Foerster LLP. Retrieved from https://www.mofo.com/resources/insights/190122 french-dpa-google-gdpr-fine.html

124