Ethics and Information Technology (2018) 20:127–142
https://doi.org/10.1007/s10676-018-9452-x

ORIGINAL PAPER

Societal and ethical issues of digitization

Lambèr Royakkers[1] · **Jelte Timmer**[2] · **Linda Kool**[3] · **Rinie van Est**[3]

Published online: 16 March 2018

Abstract
In this paper we discuss the social and ethical issues that arise as a result of digitization based on six dominant technologies: Internet of Things, robotics, biometrics, persuasive technology, virtual & augmented reality, and digital platforms. We highlight the many developments in the digitizing society that appear to be at odds with six recurring themes revealing from our analysis of the scientific literature on the dominant technologies: privacy, autonomy, security, human dignity, justice, and balance of power. This study shows that the new wave of digitization is putting pressure on these public values. In order to effectively shape the digital society in a socially and ethically responsible way, stakeholders need to have a clear understanding of what such issues might be. Supervision has been developed the most in the areas of privacy and data protection. For other ethical issues concerning digitization such as discrimination, autonomy, human dignity and unequal balance of power, the supervision is not as well organized.

Keywords Digitization · ICT · Technology · Ethics · Public values

Introduction

Information and Communication Technology (ICT) and digitization are ubiquitous in our society. ICT is also linked with other technologies, such as nanotechnology, biotechnology and neurotechnology. This so-called NBIC convergence has become increasingly visible since the late 1990s. Digitization penetrates every aspect of our lives: the technology nestles itself *in* us (for example, through brain implants), *between* us (through social media like Facebook), knows more and more *about* us (via big data and techniques such as emotion recognition), and is continually learning to behave more *like* us (robots and software exhibit intelligent behaviour and can mimic emotions). Van Est (2014) referred to this as the intimate technological revolution. The digitization of society pushes the boundaries of our abilities and offers all sorts of opportunities, but also challenges our moral boundaries. In this paper we describe what social and ethical issues arise when society becomes digitized on the basis of six dominant technologies: Internet-of-Things, robotics, biometrics, persuasive technology, virtual & augmented reality, and digital platforms.

Internet-of-Things (IoT) and robotics mainly penetrate in our *material world* (e.g., the production process, public space, and our home). IoT is based on a worldwide network that integrates the physical world with the virtual world of the Internet. Through the emergence of IoT, we are on the brink of a new era in which objects and people in the material world can be monitored, and where objects and people can exchange information automatically. In this way, the alarm clock does not just wake up a person, but at the same time switches on the coffee machine for making fresh coffee with our breakfast; or the fridge tells us a product has passed its expiry date; or the lighting in the room adjusts itself to what is happening in a video game being played at that moment.[1] Many technology companies predict that IoT will be omnipresent in our daily lives in the future. Many of the technologies we describe in this article are part of IoT: like the augmented-reality glasses which use the Internet to give users real-time additional information about their environment, or a biometric camera which can be linked to an online database to recognize faces. The development of IoT and robotics is strongly linked. Just like IoT devices,

✉ Lambèr Royakkers
l.m.m.royakkers@tue.nl

[1] Eindhoven University of Technology, P.O. Box 513, 5600 MB Eindhoven, The Netherlands

[2] Livework Studio, Rotterdam, The Netherlands

[3] Rathenau Instituut, Den Haag, The Netherlands

[1] http://www.youtube.com/watch?v=1Y3MQrcekrk.

robots are mostly equipped with sensors to read their environment; they are increasingly connected to the cloud to share and analyse data, and on the basis of those analyses, carry out independent actions. Although some issues consequently overlap, robotics triggers its own set of specific ethical dilemmas.

Over the past 6 decades the *biological world* (e.g., the human body, the brain, and our behaviour) has also been digitized by biometrics and persuasive technology. Biometric information enables the use of unique physical characteristics—such as a person's face, voice or fingerprint—for verification or identification purposes. An example of verification through biometrics is the electronic border control (e-gates) at airports. The traveller puts their passport on a reader, looks in the camera and the gate then opens or not. The identification system operates as follows: a digital image of the face stored in the passport is compared with the picture of the face taken when the traveller looked in the camera. If the biometric system—in this case a face recognition system—decides that the face stored in the passport is the same person as in the picture, the passport control system concludes they must be the rightful owner of the passport and opens the e-gate. After recognizing and analysing human behaviour, the next step is influencing that behaviour. Persuasive technology is defined by Fogg (2002) as a technology that aims to encourage people to change their behaviour. To achieve this, there should be the right motivation, the possibility to undertake action and a stimulus that induces certain behaviour. Persuasive technology is, for example, used to persuade a driver to wear a seat belt. Security is the motivation here. By sounding a signal when drivers are not wearing a seat belt, they can be persuaded to actually fasten the belt.

The growing use of ICT also means digitizing the interaction between people, as well as between people and organizations by augmented & virtual reality and digital platforms. So digitization penetrates our *social-cultural world*: shopping, transactions, listening to music, contacting friends, taking action and finding a date are things we do increasingly online. The advent of social media and other online services in the late 1990s and at the turn of the century have had a huge impact on the way we communicate. Services have acquired an increasingly important role in our culture and for forming our identity. Our lives are, for example, interwoven with our smartphone, which forms the connection between the real and virtual world. Floridi (2015) refer to this as *onlife*: the distinction between offline and online life is now completely blurred; they have become one. Recent developments in virtual reality (VR) and augmented reality (AR) also contribute to this fusion. In AR, the real world is mixed with virtual information, animation or objects. In fact an additional digital layer of information is added to our reality, for example, via smart glasses such as Google Glass. With VR, the interaction takes place in a completely virtual, three-dimensional, interactive and computer-generated environment, in which users have an artificial experience. In the future, VR could play an important role in our social lives. It will vastly expand the social media opportunities: people will be able to spend not only time with friends online but also share all kinds of experiences and adventures. Digital platforms enable smart and efficient transactions. Through these digital platforms, radically new organizational forms began to appear after 2010. Examples are Airbnb and Uber that in a few years have become major economic players, drastically disrupting their respective branches. There are plenty of other initiatives particularly in relation to the sharing economy, i.e., the phenomenon that consumers let each other have their unused consumer goods, perhaps for a fee (Frenken and Schor 2017). Another example of a digital platform is blockchain technology. This technology enables the development of so-called autonomous organizations—consisting entirely of bits and bytes. As the technology can automate a series of appointments and tasks, it can therefore take over the function of a certain organization.

Our description is not exhaustive but gives an idea of the various types of societal and ethical issues that arise as a result of digitization. At present, most of the public and political focus is on privacy issues (especially personal data protection) and digital security. The major challenges are the search for digital inviolability of the home and the protection of privacy with the emergence of IoT. We also see a growing focus on issues like justice and the balance of powers. Regarding the former, the focus is on big data, algorithmic profiling, the impact on the right to equal treatment, and presumption of innocence. The dominant position of large internet companies is becoming a hot topic of debate with regard to the balance of powers. Autonomy, human dignity and control of technology are still less popular topics in the public debate and are only being flagged up to a limited extent by social organizations and in policy-making and provision circles. Consequently, these are the areas where we identify blind spots in the governance landscape. We are therefore conducting an ethical technological assessment from the perspective of digitization, and that digitization and the ensuing social and ethical issues will find their way to the social and political agenda.

Our analysis of the scientific literature on technologies revealed several recurring themes: privacy, security, autonomy, justice, human dignity, control of technology, and the balance of powers. We have applied these themes to structure our discussion in this paper. The various ethical and social issues manifest themselves per technology in different ways. Privacy, for example, takes on a whole different meaning in the context of IoT than in the context of biometrics. Not every theme is explored in depth for every development; we focus on the distinctive issues that a particular

technology demonstrates within the overarching trend of digitization. Finally, our summary in the conclusion shows which ethical and social issues have explicitly put the new wave of digitization on the map. We briefly indicate how the issues in this paper relate to important values as laid down in international treaties.

The research to describe the ethical and societal issues raised by digitization was done by carrying out a literature review.[2] The scientific literature, mainly, from 2010 was investigated for each area of technology, using search engines such as Google Scholar and Scirus as well as the PiCarta database. Combined with the term for the technology (or related terms and synonyms of this technological field), we entered the following search terms for each area of technology: ethics, ethical, moral, morality, normative, or normativity. Based on the finding publications, we describe the most urgent and problematic ethical and social issues per technology mentioned in the literature. In addition to scientific publications, the desk review included consulting all kinds of newspapers and news sites to illustrate certain issues based on compelling reports in the news.

Societal and ethical issues

Privacy

Digital home

Through IoT, more and more information about ourselves is being exchanged, without us really knowing or having control over it (Barbry 2012; Peppet 2014; Roman et al. 2013). Samsung's 46-page privacy policy that comes with its smart TV, tells you that Samsung registers where, when, how and what time you have your TV turned on. The TV also has a camera for face recognition and a microphone for speech recognition. Samsung's manual warns you to watch out what you say in the vicinity of the TV: "Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party." This led to quite a fuss (Gibbs 2015). The example shows that permission is given unwittingly to use certain data, because people are not able to understand the entire manual or are suffering from so-called *consent fatigue* due to the large amount of permissions they have to grant about using data that devices capture (Pereira et al. 2013). This raises the question of where the responsibility lies in this process: should the user be expected to sift through the conditions for each and every device? Or do the manufacturers of all these devices also bear some responsibility? Should they not ensure a certain reasonable expectation of privacy?

Because of IoT, we can in fact be followed everywhere, which can lead to huge transparency at the expense of our privacy. In most cases, the data collated by smart toothbrushes, thermostats, televisions, refrigerators and washing machines are the property of the manufacturer, not the user. The home, which we consider to be our private domain, is thus becoming transparent, because processes in the home can be monitored via the IoT devices inside our houses. The distinction between home and the outside world is blurring as the walls and curtains no longer protect the house against prying eyes. That is why Koops and Prinsen (2005) argue for protecting citizens against this digital spying and for providing citizens with digital privacy alongside physical privacy in the home. This should ensure protection against observation from outside with technical aids, so that citizens have a place where they can pre-eminently be themselves.

Pervasive monitoring

Just like the IoT, robots contribute to the increasing potential for collecting data in situations where formerly no (digital) data collection took place. Robot technologies can be deployed in a variety of ways to monitor certain situations, such as a patient's wellbeing, a car driver's state of mind or the safety situation on the street. As a direct result, robot technologies can invade our privacy in all sorts of ways. Robots and domotics, for example, can monitor people, record and pass on details of their physical condition, and even enable a care recipient to be watched 24 h a day. As this data provides a great deal of information on the care recipients' daily ups and downs, it thereby raises issues about their privacy. Care recipients will not appreciate, for example, that it is recorded when they are not yet dressed or about to have a bath. This issue is more complex when it comes to older people with dementia: to what extent can they show whether they are aware of the presence of a technology that captures their daily lives (Borenstein and Pearson 2010)?

Privacy enhancing versus losing control of sensitive information

In relation to privacy, biometric technology is a double-edged sword. It can be used to protect privacy, whereby only the minimum amount of information is required to determine whether someone is entitled, for example, to enter a building or to buy alcohol. On the other hand, because biometrics can identify sensitive information, controlling what happens with that information may be tricky, especially now that the technology has reached the stage of being applied in many more devices and situations.

[2] We are indebted to Luca van der Heide for collating the specific literature for this review.

In the above example of the e-gates, biometrics is implemented in such a way that privacy is guaranteed. The identity of the user is not released, only authentication takes place: is the face in front of the camera the same face as in the passport? Verification can also be done by comparing someone's biometric characteristic with the information already stored about that person. For example, if wine shops make use of a biometric fingerprint system to verify that someone is older than eighteen, all they need to know is that the information in the fingerprint belongs to someone over the age of eighteen. The name of the customer is not important. Thus biometrics can be a good way to prove legitimacy while maintaining privacy.

Other applications of biometrics are particularly aimed at identification and recognition (Kindt 2013). For example, someone's facial profile is compared with a database to see if the scanned person appears in that database. The technique is applied in police investigations or for security cameras in public spaces. This use is regulated by law; importantly, such highly sensitive information must be stored safely and securely. The biometric data can namely contain information about the user's health and ethnicity (Juul 2013). It could be undesirable that, for example, an insurance company or employer gets a hold of the information. This problem is aggravated by the fact that modern biometric identification methods can also find indications of a person's health risks. An iris scan can, for example, determine diabetes or high blood pressure. Irregularities in fingerprints may indicate leukaemia or breast cancer.

Recent years have seen huge advances in biometrics. The presence of large databases with photos, the accessibility of software, and the ubiquity of cameras in smartphones, ensure an uptake of facial recognition technology in an increasingly wider range of situations (Janssen et al. 2015). Scientists showed that by using facial recognition technology and public data in Facebook profiles, they could identify a third of the students on a university campus (Acquisti et al. 2014). The fear is that accessible facial recognition technology could ultimately lead to a situation where it is no longer possible to walk down the street anonymously. The app FindFace, which was launched in Russia in 2016, allows users to compare a picture they have taken of someone on the street, with profile photos on Vkontakte—the Russian counterpart of Facebook—in order to discover someone's identity. "If you see someone you like, you can photograph them, find out their identity, and then send them a friend request," according to one of the app's creators (Walker 2016).

The next generation of biometrics not only gives insight into "who you are" but also focuses on the question "how you feel" (Mordini et al. 2012). Emotion recognition technology, for example, gives insight into people's state of mind, and can even be used to expose emotions that people try to hide, by examining people's unknowingly automatic non-verbal comments (Dwoskin and Rusli 2015). This is an invasion of a new field of privacy, namely "mental privacy". We are talking about people's right and ability to keep private what they think and feel. In addition to facial expressions, other forms of behaviour can be analysed. Certain ways of walking, grimaces and other facial expressions can reveal something about a person and their behaviour. The extent to which a person has control over whether they submit the above data seems to be limited, as the collection of this information can be done remotely and covertly, for example, by inserting facial recognition technology in mannequins,[3] without the knowledge of the person being observed (De Hert and Sprokkereef 2012).

Little Brother and misuse of virtual avatars

A hotly debated development in AR is Google Glass. Launched in 2013, this portable computer designed in the shape of a pair of glasses, projects information onto a small display in front of you. In early 2015, Google stopped manufacturing Google Glass as a consumer product for the time being in order to focus on business applications.[4] One of the reasons why the public launch of Google Glass floundered was because of so much public unrest concerning the possibility to film private conversations and social interactions (unsolicited) with the glasses. The development of AR is causing concerns about a so-called 'Little Brother' scenario: instead of a government spying on everyone, citizens and companies are the ones spying on each other continuously. Smart glasses or lenses are ideal for tracking people and spying on them without people being aware of it (Geser 2010). Especially if such AR glasses or lenses are equipped with a face recognition app, the user gets real-time information about the person in front of them. The glasses thus enable the wearer to register all sorts of things without others seeing that registration is taking place. The fact that this is against the law will probably not hinder attackers, because it is almost impossible to trace them.

In addition, the smart glasses or lenses raise yet another issue: who owns the images that the glasses record? In other words: does the wearer of the smart glasses or lenses have exclusive rights to his/her own observations (Brinkman 2014; Wolf et al. 2015)? Google applied and obtained a patent for the technology that enables the company, by following eye movements, to see what the person wearing Google

[3] http://www.wired.co.uk/news/archive/2012-11/23/mannequin-spies-on-customers.

[4] http://www.theguardian.com/technology/2015/jul/31/google-glass-wearable-computer-businesses.

Glass is looking at.[5] In this way the company not only has at its disposal the image that the wearer of glasses sees, but also obtains information on precisely when and what the wearer is looking at. Other companies that record images can make very good use of this data for profiling and thus incorporating it in their business model.

The issue with privacy in VR concerns the new ways of tracking people's behaviour in virtual spaces. Games manufacturers like Knack[6] demonstrate, that from the way someone plays a game in the virtual world, we can learn a great deal about their personality, how they interact with others and how they solve problems (Peck 2013). The more that social interaction shifts to social networks in VR—Facebook's aim—the greater the impact on privacy. In addition, continuous monitoring can lead to social conformism, reduced authenticity and self-censorship (O'Brolchain 2016).

Insight in all platform interactions

The issue of privacy also applies to digital platforms. The platform administrator can track all the transactions and interactions that take place within the platform and many of these transactions contain sensitive information. Platforms can easily track their users with simple tools. In particular the way Uber (employees) dealt with the privacy not only of their drivers but also of their customers, caused quite a stir (Rogers 2015). It was reported that Uber used their so-called 'God View' real-time tracking system on customers as well as drivers. An Uber employee's blog post, which incidentally has been removed, bragged that, based on the data they collect, Uber can assess which of their customers has had a one-night-stand. They can draw this conclusion when two different customers are dropped in the evening at an address where neither of them lives, and are picked up in the morning and then each taken to their own address.[7] After reaching a 20,000 dollar settlement with the department of justice in New York, Uber tightened up their privacy policy. 'God View' has since been anonymized and the number of employees that can access drivers' personal information has been reduced. In addition, the location data for the Uber drivers and customers is encrypted.[8] This data can still, however, be viewed with a password known to Uber. Strict surveillance of privacy guidelines for platforms that have a tendency to evade regulations, seems badly needed. In this way, it can be clarified what data is collected, how it is collected and used, and whether it is resold (Scholz 2016).

Autonomy

Technological paternalism

IoT does not just offer us comfort, but can also lean towards technological paternalism (Hilty 2015). We speak of paternalism if someone professes to know better what is good for other people than these people themselves. With technological paternalism, the paternalism is 'delegated' to technology. A smart fridge is technologically capable of changing the order for your favourite cheese to a low-fat cheese because the biometric sensor has measured that the particular person's cholesterol levels are too high. The question is, however, whether the fridge and the biometric sensor should be allowed to make such a decision together. This kind of technological paternalism has serious ethical implications for IoT: the implicit enforcing or provoking of certain behaviour can endanger personal autonomy. What is more, IoT can thus be implemented as persuasive or even manipulative technology.

Control and manipulation through technology

The most prominent ethical issue that imposes itself on persuasive technology is that of human autonomy: to what extent may we influence people and when can we apply this technology? According to Smids (2012), persuasive technology should comply with the requirement of voluntariness to guarantee autonomy. An action is only done voluntarily if the action is done intentionally (the one acting is 'in control') and is free from controlling influences. For example, if someone does not want to wear the seat belt and hears a constant beeping sound, they are being subjected to a controlling influence—in this case a kind of coercion. The driver can only stop the irritating sound by fastening the belt. Besides this coercion, there are examples of manipulation of controlling influences (such as withholding information or deception) and excessive stimuli (for example, a massive reward).

Ideally, persuasive technology aims to halt temptation, and have the user independently display the 'desired' behaviour. In that case, persuasive technology is training the user.

[5] http://www.patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.htm&r=36&p=1&f=G&l=50&d=PTXT&S1=%2820130813.PD.+AND+Google.ASNM.%29&OS=ISD/20130813+AND+AN/Google&RS=%28ISD/20130813+AND+AN/Google%29.

[6] Knack produces so called *assessment games*, computer games designed to test people's performance in a work situation.

[7] http://www.whosdrivingyou.org/blog/ubers-deleted-rides-of-glory-blog-post.

[8] http://www.buzzfeed.com/johanabhuiyan/uber-settles-godview#.yvb4dKlNR.

The purpose of training someone is that they can function independently and no longer need guidance. Unlike training, manipulation aims to keep someone dependent. According to Spahn (2012), persuasive technology should be training not manipulation, and eventually make itself superfluous. An important condition for this is that the user shares the same goal of the intended persuasion. If a user wants to drive more sustainably, she will warmly embrace any attempt to help her achieve her goal. If the user does not share this goal, then an additional motivation can provide a solution, in this example by pointing out that it is financially attractive to drive sustainably.

Technology that triggers behaviour in a more compelling way is, however, not necessarily undesirable. Firstly, people themselves can opt for compelling technologies. Some people are very pleased with the peeping sound that a car makes if it is too close to another vehicle or object, for example, when parallel parking, or with rest break software to prevent RSI with programmes that compel you to take a break. People decide for themselves, by not switching off these systems, to depend on this technology. Secondly, compelling technologies could be used if the individual's behaviour can lead to a collective risk. Some people advocate mandatory speed limiters in cars, which restrict individual freedom but reduce the collective risk of other road users.

As we have seen, persuasive technology can also feature in smart IoT environments. This means that influencing becomes part of the environment and in some instances occurs less consciously. This is the case when subtle feedback is given on ambient lighting (Maan et al. 2011), whereby the 'nudging' takes place at a low cognitive level without the user being aware of it. Such forms of persuasion may constitute a threat to the individual's autonomy if behaviour is controlled without the individual knowing or being aware of it. Transparency and insight in the way persuasive technology is applied are therefore important factors for protecting autonomy.

Steering preferences

When a smart IoT environment anticipates our needs and wants, a choice is made about our supposed preferences—for example, suggesting a selection of certain TV programmes—based on previously displayed behaviour. With that choice, the smart environment sorts our options and steers us in the direction of certain choices and behaviour. The way subtle changes in our behaviour can be accomplished through technology became apparent from the Facebook emotion experiment in 2014. By adapting the number of positive and negative messages in users' *newsfeeds*, they were able to influence users' state of mind without them being aware of this (Kramer et al. 2014).

Hildebrandt (2012, 2015) puts forward that a future generation of technology could be so sophisticated in reading our preferences, that it detects preferred choices before we ourselves are even aware of them. She outlines the scenario of a smoker: someone profiled as almost wanting to stop the habit, but has not yet consciously made that decision; they are subsequently targeted via ads and news reports criticizing the negative effects of smoking, to steer them in a different direction. According to Hildebrandt, providing transparency in the profiles on which automatic decisions are based, is an essential condition to protect the autonomy of the individual.

'Man out-of-the-loop'

In robotics we see a shift "from *in*-the-loop to *on*-the-loop to *out*-of-the-loop" (Sharkey 2010), which is also noticeable in IoT. In-the-loop means that the person is in control and human permission is required to have the system carry out an action. On-the-loop means that the person makes a decision based on information in the system. Out-of-the-loop refers to a situation of full automation, where the system makes a decision without human intervention. The shift from *in* to *on and out of* the loop has occurred due to the increasing amount of information from various sources/devices that has to be integrated and subsequently interpreted to come to a decision. Robots can do this far more efficiently and effectively than humans, for whom it is almost impossible. As a result, people in fact no longer make the decisions themselves but leave it to technology. Examples include knowledge systems that make medical diagnoses based on a large amount of information, military robots that take life or death decisions using information from various sources, and the driver support systems that decide what speed we should drive on a particular stretch of road. It raises the question of how these systems come to their decisions and if the competitor's software would make the same decision.

Due to the huge advances in artificial intelligence, robots are becoming more and more autonomous. The crucial question is: to what extent is it ethically acceptable to delegate the responsibility for moral decisions to robots? This is an ongoing debate in the field of military robots and self-driven cars. According to Arkin (2010), the military robot will surpass humans when making moral decisions, because human soldiers undergo tremendous stress in the battlefield, and robots—free from stress—make fewer mistakes. The problem here is that robots cannot be called to account, and for many scholars, that is the reason why robots should never be allowed to make life and death decisions.[9]

[9] When the International Committee for Robot Arms Control (ICRAC) organized an expert workshop 'Limiting Armed Tele-Operated and Autonomous Systems' in 2010, the majority of the attend-

The same problem occurs with self-driven cars. Traffic accidents are inevitable, also with a self-driven car, and so this car will experience situations that require a moral decision (Goodall 2014). In such a situation, a human driver acts instinctively; It is impossible to expect him in half a second to make a well-considered choice between driving into a truck or mowing down a child on the pavement. For a self-driven car, however, half a second is more than long enough to asses various scenarios. Should the car choose the least injury to the occupants of that car or, for example, for the least total damage, thereby also taking other road users into account? The question we need to ask before this issue arises is: Do we leave this moral decision to the self-driven car, or do we determine beforehand what this car should decide in situations where it cannot avoid an accident?

Filtering and freedom of expression

Online platforms play an increasingly greater role in determining what information and what news people see. A well-known example is how different persons' Google search results vary because of a personalization algorithm that looks at things such as previous searches (Pariser 2011). Algorithms used to be deterministic—the programmer determined beforehand an action for every situation—and it was possible for someone to figure out how the algorithm came to a decision. Through systems like artificial intelligence, algorithms do not follow a predetermined set of rules but make use of self-learning statistical techniques. As a result, the decisions that an algorithm makes are almost unfathomable and uncontrollable for humans (Pasquale 2015; Scholz 2017). To prevent manipulation, it is therefore crucial that we understand why such algorithms make certain choices, and how to implement transparency (Turilli and Floridi 2009). Research by psychologist Robert Epstein showed that search results can greatly influence voters' preferences by changing the order of the results in a search engine, such as Google. According to Epstein, this represents a serious threat to democracy.[10] This raises questions about the steering role of major platforms and also about freedom of expression. A recent example is when Facebook removed the iconic and harrowing 1972 World Press Photo of a girl fleeing from a napalm attack (the 'napalm girl' as the picture would later be called). Following widespread criticism, Facebook later reversed its censorship decision and reinstated the photo.[11] Other platforms like Google and Twitter (not forgetting Facebook), have been criticised for facilitating the spreading of 'fake news'.[12] This has led to a debate on the role and responsibilities of platforms in relation to freedom of speech and filtering information. In the aftermath of the 2016 US presidential elections, this debate triggered a great deal of controversy. The platforms are examining what action they can take against fake news.[13]

Security

Information security gets a physical dimension

Digitization also presents serious crime problems: the Internet or the devices connected to the Internet can themselves be the target of crime, as is the case with hacking or DDoS (Distributed Denial of Service) attacks which paralyse websites or systems. Experience shows that virtually any digital system can be hacked. In 2012, for example, researchers at the University of Texas demonstrated to the US Department of Homeland Security how relatively simple it was to hack into and take over control of a military drone.[14] To do this, they used the technique known as *spoofing*: obtaining unauthorized access to a device by forging the identity of the person controlling the device. There is indeed a fear of cyber-terrorism in policy circles.

Hackers can also gain access to sensitive information, and that information could end up in the hands of the wrong people. A hacked smart meter could give burglars insight in the exact times of the day or week when we turn the heating down and are—evidently—absent. Besides extracting information that is valuable to them from smart devices, criminals can take over the control of smart devices. This adds a physical dimension to the issue of security. A security researcher demonstrated how simple it is to hack the toy doll Cayla, and have it quote passages from the erotic novel *Fifty Shades of Grey* and from the fictional psychopath Hannibal Lecter in the book *The Silence of The Lambs*.[15] The hacking of the doll is a relatively harmless example, but New Zealand hacker Barnaby Jack showed at a conference in 2011 that he could hack his friend's insulin pump. He could take complete control and was able to administer a fatal amount

Footnote 9 (continued)

ees signed a statement emphasizing the necessity that a human being must always make life and death decisions (http://www.icrac.co.uk/Expert%20Workshop%20Statement.pdf).

[10] http://www.politico.com/magazine/story/2015/08/how-google-could-rig-the-2016-election-121548.

[11] http://www.bbc.com/news/world-europe-37721193.

[12] http://www.reuters.com/article/us-twitter-facebook-commentary-idUSKBN13W1WO.

[13] http://www.nytimes.com/2016/11/15/technology/google-will-ban-websites-that-host-fake-news-from-using-its-ad-service.html?_r=1.

[14] http://www.bbc.com/news/technology-18643134.

[15] http://www.mirror.co.uk/news/technology-science/technology/friend-cayla-doll-can-hacked-5110112.

of insulin. Other hackers have also already pointed out that they could take control of a wireless pacemaker and have the device deliver a fatal shock (Greenberg and Zetter 2015).

The issue of security is becoming even more complicated because of the fact that IoT devices are connected to each other. So, for example, successfully hacking a coffee machine can give you access to a car or open the front door. In addition, this type of security issue is new for many manufacturers of consumer electronics, which means it has not always been given much thought. As hacker Runa Sandvik neatly surmised, "When you put technology on items that haven't had it before, you run into security challenges you haven't thought about before" (Greenberg and Zetter 2015).

Identity fraud

Identity fraud is a major social problem that will probably only increase in scope (Sandhya and Prasad 2017). Identity fraud is the intentional obtaining, appropriating, owning or creating of false identifiers, thereby committing or intending to commit unlawful conduct. Advanced biometrics has to reduce identity fraud. Passports nowadays have a chip with a facial scan and digital fingerprints. In the United Kingdom they use iris scanning. Besides the frequently mentioned convenience for users, biometric recognition also has the advantage from a security point of view that the user must be physically present. This reduces the risk of fraud by means of falsification of documents, theft of cards and revealing of passwords.

However, biometric technology is not infallible (Heimo et al. 2012): biometric systems can be misled with falsified elements, for example, by means of spoofing: falsifying characteristics in order to assume a false identity temporarily. In this way German hackers showed that by using a couple of photos—such as those of a press conference—they could forge the German Minister of Defence's fingerprint (Hern 2014). Another disadvantage is that in case of biometric identity theft, no other fingerprint or facial profile can be made, unlike being able to request a new password. Less sophisticated methods of detecting identity fraud also led to the first horrific scenarios with securing fingerprints. In a car equipped with a fingerprint reader, during a car theft, in order to disconnect the security, the owner's finger was cut off, so that the perpetrators were able to drive off in the car.[16] Instead of consisting of mere information about persons, also a proactive understanding of biometrics is needed to consider the ways in which this 'informatization of the body' may eventually affect how people use their bodies and experience space and time (Hayles 1999; Van der Ploeg 2007).

[16] http://www.news.bbc.co.uk/2/hi/asia-pacific/4396831.stm.

Safety: psychological damage in virtual worlds (VR)

German philosophers Madary and Metzinger (2016) focus on the risks of VR technologies that give users the feeling they are in a different body to their own and particularly in situations where users interact with other virtual or real people. In these situations, unethical behaviour occurs which has already led to controversy with computer games (Seddon 2013). A well-known example is that someone reported that her avatar was apparently indecently assaulted in the computer game Second Life. According to Madary and Metzinger (2016), the emotional involvement within a virtual environment in which we are *actually embodied* is much greater. That means that the psychological damage that someone incurs as a result of an indecent assault in virtual reality, will probably be much greater than previous cases in the game Second Life (see also Kizza 2013). It is expected that in the near future, people will visit each other more often in virtual environments and that social networks such as Facebook will also support these possibilities.

Balance of power

Everything-as-a-service

IoT devices are often offered as part of or in combination with a software service. Thus the sale of a smart TV or smart refrigerator can include software support. The product's capabilities are for the most part embedded in the accompanying software. Thus the ability to have the refrigerator in the morning display the schedule for the following day, depends on the manufacturer's software support. The manufacturer can decide to stop offering support for older appliances, rendering them partially or entirely useless. The Electronic Frontier Foundation raised the alarm because consumers, having forked out hundreds of dollars for a smart home console with lifetime software support, were suddenly left with a worthless product because the support was removed after a competitor took over the company (Walsh 2016).

When products become more dependent on software controlled by the manufacturer, this strengthens the manufacturers' control and how that can be utilized. In addition, there is a noticeable trend that the products themselves are being offered as services. This is called 'servitization': consumers no longer buy light bulbs but purchase light as a service, they do not purchase a washing machine but make use of washing services, etc. The manufacturer is responsible for the maintenance of the appliances, consumers only need to pay a periodic fee. Proponents advocate the convenience that such services provide, whereas opponents see consumers' control of their own environment dwindling; it is, for example, no longer possible to unscrew or adjust something

yourself. The manufacturer retains ownership and can decide to change the product in some way whenever they like. A case in point is when Amazon decided to remove from customers' eReaders certain eBooks by George Orwell, notably the author of the work 1984, due to a conflict with the supplier about copyrights. Amazon was allowed to do this, because customers did not officially purchase the books, but had them on loan from Amazon (Stone 2009).

Who sets the standards?

In relation to persuasive technology, a user is not able to engage in a discussion with the technology like they can with a human interlocutor. That makes for an asymmetrical relationship in this communication: the standard is set in the technology, and the user is unilaterally exposed to it. Spahn (2012) therefore argues that it is important that the user has as much influence as possible on how this standard is determined, and consciously agrees to applying persuasive technology. If a user decides to purchase a digital fitness coach, we can assume this is of her own accord. However, when persuasive technology is used in the context of a working environment or in insurance, this issue becomes more problematic (Timmer et al. 2015). It raises the question of whether the employer or insurer should be allowed to determine the standards for an employee or client's behavioural change, or if this is an infringement of their personal autonomy. The Dutch data protection authorities recently ruled on the application of wearables by employers for gathering personal information,[17] but there is still no ruling on whether employers may implement wearables for steering behaviour.

Unfair competition and monopolisation

According to Scholz (2016), certain platforms' success is not only due to the technological possibilities, but is to do with the companies concerned applying 'illegality as a method'. This leads to unfair competition between platforms and regular companies, because platforms do not (have to) stick to the rules or permits that apply to regular companies. Airbnb enables individuals to let rooms without a licence, and does not have to fulfil the same safety and tax liability requirements as regular hotels. UberPop drivers do not have to keep to the driving and rest periods, nor comply with the same safety regulations as taxis, and they do not need to charge VAT. On the other hand, the average UberPop driver earns less than the minimum wage and most drivers see this as a part-time job.[18]

Frenken et al. (2015) think that a tolerance policy is initially logical in order to give experiments space and to assess the effects. However, the authors advocate clear legislation as platforms like Airbnb and Uber are growing so quickly that they have a disruptive and unexpected impact on existing sectors and on society as a whole. Such platforms can be concentrations of power, with monopolies consequently yielding high profit margins. These monopolies can exist because the platforms typically benefit from network effects as we have seen with internet companies like Google (internet searching), Facebook (social networking) and WhatsApp (mobile messaging). Whatsapp, for example, only works if there is a large network of users. Once an app like this becomes the largest, competing with it is almost impossible because of what we call 'the winner takes all' (Kreijveld et al. 2014). Kreijveld et al. state that it is relatively easy for platforms to expand their scope by integrating and adding new services (like Uber, that is now working on package delivery),[19] which begs the question whether such platforms are not getting too big. One consequence is that users become dependent on such a platform, because it is a hassle to use a different platform where the network is too small and therefore not interesting. Accumulated data and connections within a platform as well as other services associated with the accumulated profile also make it difficult for a user to move to another service – the so-called '*lock-in* effect' (Parker and Van Alstyne 2017). .

Relations between private and public parties

The 'public space' on the Internet—consisting of things like social networks—is mostly in private hands. All the interactions that take place in that pseudo-public space are therefore the property of the platforms, and the information generated in this way can be used or resold as required. Also the conditions for interactions taking place, and what statement may or may not be desirable, can be changed by the platform administrator at will. There has been a lot of controversy about Facebook's decisions to remove certain statements from the platform. Critics argue that the current situation is leading to a form of *digital feudalism* (Meinrath et al. 2011; Balkan 2016; Zuboff 2015; Helbing et al. 2015); a situation in which people's ownership of themselves—their digital representation—is lost.

Governments are also gathering more and more data about citizens. Helbing et al. (2015) describe a future

[17] http://www.autoriteitpersoonsgegevens.nl/nl/nieuws/ap-verwerking-gezondheidsgegevens-wearables-door-werkgevers-mag-niet.

[18] http://www.volkskrant.nl/economie/uberpop-chauffeur-haalt-vaak-minimumloon-niet~a3823583.

[19] http://www.rush.uber.com/how-it-works.

scenario of *big nudging*, with authorities using data to steer citizens' behaviour. The most striking example is the Chinese Government: for each of its citizens it keeps a *citizen score*, which plays a role in determining whether someone is eligible for a loan, a visa or a job. Government data collection is causing increasing information asymmetry between citizens and governments, with citizens becoming more transparent and governments becoming less transparent for their citizens.

Human dignity

Dehumanization and unemployment

Although robotics can provide great support in health care, entertainment, the police and the army, if the technology is not applied within certain framework conditions, it can undermine human dignity. We are talking about the risk of objectification or instrumentalization of people, in other words dehumanization. The health care sector seems to be anxious about the implementation of robotics. The way robots are deployed seems the crucial fear. Coeckelberg (2010) argues that care robots should only be used for 'routine care tasks'. That means tasks for which no emotional, intimate, personal involvement is required. If robots are deployed to replace the caregiver, there is a risk that care is dehumanized (Sharkey 2014). When robots take over tasks such as feeding and lifting, the care seekers can feel like objects. The ethical complaint about 'objectification' ties in with the idea that robots cannot provide care. The underlying argument is that robots are devices which are not able to replicate the empathic capacities and reciprocity of human care relationships. Human contact is usually found to be essential for providing good care. The patient's quality of life should therefore be the guiding principle for robotics in healthcare (Van Wynsberghe 2015).

There is also a risk of dehumanization in other areas of care. Soldiers who control armed robots remotely, are not present in the danger zone. In such a situation, the use of tele-guided robots creates an emotional, and therefore also moral, distance between the action and the ethical implications of that action. Proponents argue that this can reduce psychological suffering among soldiers and ensure decisions are more rational.[20] Critics fear that the danger lurking in creating more distance between an action and its consequences, is that controllers make important, sometimes life or death decisions, as if they are playing a video game. Tele-guided armed robots can heighten the risk of dehumanizing the enemy and desensitizing the controller (Royakkers and Van Est 2010).

Another aspect that has led to a great deal of discussion in recent years is the potential impact of robotization on employment. Robots are not only capable of supporting human tasks, they can gradually replace more and more human tasks and therefore also jobs. Two opposing views dominate this discussion on the effect of automation: on the one hand robotization leads to economic growth, employment growth (new jobs are created) and an acceptable distribution of wealth; on the other hand, robotization leads to fewer jobs and consequently declining prosperity.[21]

Instrumentalization and the standard user

Biometric systems can give both 'false negative' as well as 'false positive' results. You get a 'false negative' result when the identification device does not recognize an authorised person. This need not be a problem if they can immediately try again to identify themselves. But something like this can also cause a great deal of inconvenience. For example, a motorist in the United States had his licence taken away because the facial recognition system mistook him for another person. It took 10 days of bureaucratic wrangling before he could prove who he was and finally get back his licence.[22] This example shows that the use of biometric systems can lead to instrumentalization of the individual, thereby reducing the individual to a data point in a system. The user-friendliness of biometrics is great if the system works well for people. But for those who are incorrectly identified as suspicious by the system, it is often very difficult to rectify errors. In addition, it appears that biometrics cannot be used for everyone. Two percent of people's fingerprints cannot be 'read' because they are senior citizens or because of certain chemotherapy treatments (Renaud et al. 2015). This kind of problem occurs in many digital systems: they are designed on the basis of particular standard user characteristics, which means they are not always accessible to people who do not conform with these criteria, for example, because their name does not match the system, or they have changed gender.

Unlearn moral skills

One objection to persuasive technology is that users' actions have nothing more to do with ethics: they make no moral decisions but simply display controlled behaviour (Spahn 2013). A driver support system that constantly warns us if

[20] Although fighting from behind a computer is not as emotionally potent as being on the battlefield, killing from a distance remains stressful; various studies have reported physical and emotional fatigue and increased tensions in the private lives of military personnel operating the Predators in Iraq and Afghanistan (see, e.g., Lee 2012).

[21] For an extensive study on this topic, see Van Est and Kool (2015).

[22] http://www.schneier.com/crypto-gram/archives/2011/0815.

we are driving too fast can be very effective in terms of safety, but the risk is a certain reduction in standard awareness. Persuasive technology is potentially a powerful regulatory tool, but the moral issues call for further consideration of applying it as technical regulatory instrument. Critics paint a doom and gloom picture of persuasive technology creating a society whose citizens are controlled to behave according to the norm, without sensing that norm themselves. Internet critic Morozov (2014) therefore makes the case for technology that stimulates people's deliberative capacity (the ability to gather information and consult with other people and exchange arguments), and encourages reflection leading ultimately to behavioural change. A smart car prompts the user to drive more economically, but not to think about leaving the car in the garage for a day. In Morozov's opinion, persuasive technology should therefore encourage us to do the right things.

Desocialization and alienation

VR technology defies the usual distinction between virtual and real worlds. This arouses the fear that at a certain moment, people can no longer distinguish 'real' from 'fake'. Melson et al. (2009) fear that the massive use of these technologies will replace our interaction with nature. As a result, we will also miss the healing and creative power of nature. Louv (2005) speaks of the *nature deficit disorder*. Madary and Metzinger (2016) even voice the danger that frequent VR users will regard the real world and their body as unreal, and that their sense of reality shifts exclusively to the virtual environment. They end up neglecting their actual physical and social environment.

As far as shifting social contacts to the virtual world is concerned, Turkle (2011) is afraid that people will lose their social competencies—like dealing with rejection and settling arguments—if we have predominantly virtual contacts in the future.[23] Turkle's fear for this loss is based on her lengthy research into the influence of social media and mobile phones on communication between young people. Turkle argues that the younger generation is much less empathetic than its predecessors were, because intimacy can be avoided and therefore relationships through social media or VR are less binding. Dotson (2014) even envisages a future in which we have contact with virtual people. In his opinion, this will contribute to an undesirable shift in the collective view of 'authentic sociality'. A small group of Japanese men, nicknamed Otaku, already indicated that they prefer a virtual girlfriend to a real relationship: "With real girlfriends you have to consider marriage. So I think twice about going out with a 3D woman" (Rani 2013). Another risk, according to O'Brolcháin et al. (2016), is that VR can be addictive, just as the virtual world has produced other addictions. Gambling and pornography are constantly available through the internet, thus allowing for new online forms of addiction.

Justice

Classification and the presumption of innocence

The application of biometrics can result in misclassification and stigmatization, by automatically putting someone in a certain category, such as a terrorist, criminal or unreliable individual. This can lead to a reversal of the presumption of innocence. Biometric systems can cause someone to be considered a criminal until evidence to the contrary is furnished. It is highly likely that this stigma will stick with such a person, for example, because the presumption is stored in a database (Sutrop and Laas-Mikko 2012; Sutrop 2010). This could be reinforced by facial recognition, which makes it easier to figure out a person's identity. Thus the stigmatization of a person can take place without that person knowing about it. In the name of national security, it is only a small step to *function creep* meaning technology will be used for a different purpose than originally intended (Tzanou 2017).

Exploitation and exclusion

Platforms ensure that users have a dual role: as producers and as consumers. In this context, they are called *prosumers*. The power of platforms is that they bring supply and demand together in an efficient way, and via smart assessment mechanisms, they create the confidence that enables transactions such as renting out an apartment to an unknown person. To be able to respond efficiently to the changing demand, platforms often have a flexible team of providers who are available on demand. For this reason we refer to an *on-demand economy* (Scholz 2016). The fact that providers offer their services on call and are not employed on a permanent basis can put pressure on traditional mechanisms of employee protection, with the lurking risk of exploitation. We see that Uber drivers' working days are too long and they have little input if the company decides to adjust the fare rates (Rogers 2015).

At the same time, platforms can decide unilaterally to deny a user access to the platform. For users who depend on access to the platform for their income, this can have far-reaching consequences. Current case histories moreover show that platforms have no qualms about excluding certain users. Uber drivers may not have a rating lower than 4.6 stars (4.8 stars is average). Otherwise they can be removed from the service. Rogers (2015) describes how the continuous review system means that providers must always be friendly and cheerful. In addition to their physical work, they are

[23] See also Sullins (2012).

Table 1 Social and ethical issues evoked by digitisation

Theme	Issues
Privacy	Data protection, spatial privacy, mental privacy, Little Brother, pervasive monitoring, transparency
Autonomy	Freedom of choice, freedom of expression, manipulation, paternalism, controlling influences
Safety and security	Safety of information, identity fraud, physical and psychological safety
Balance of power	Unfair competition, exploitation, relation citizen-government-industry, accountability, control and transparency of algorithms
Human dignity	Dehumanization, instrumentalization, *deskilling* (unlearning skills), desocialization
Justice	Discrimination, exclusion, equal treatment, stigmatization, function creep

expected to perform certain 'emotional labour'. Regular taxi drivers are free to sit behind the wheel with a grumpy face, whereas for Uber drivers, that could mean losing their source of income.

Discrimination and unjust exclusion

Automated systems harbour a risk of wrong judgements. Several studies warn against wrongful exclusion and discrimination by automated systems (Zarksy 2013; Podesta et al. 2014; Citron and Pasquale 2014). Profiling puts people in certain categories, each of which is handled differently. From a service point of view, this can offer convenience and customization. But if it causes certain (groups of) people to be structurally disadvantaged, that is problematic. It appeared that female jobseekers were shown advertisements for senior posts, served by Google, less frequently than men with a similar profile (Datta et al. 2015). Even if no data about race or religion is used, other strongly correlating variables can still cause discrimination to occur (Hildebrandt 2016).

A profile that sticks to someone on account of their behavioural history, can affect their options for the future. That can lead to a self-fulfilling prophecy: someone with a good credit score finds it easier to secure a loan and to work on their financial future, whereas someone who poses a higher risk and has to comply with stricter conditions is therefore more likely to land in trouble with repayments (Citron and Pasquale 2014). The Dutch Data Protection Authority warns of 'digital predestination',[24] the danger that people can no longer 'escape' from the digital profile established about them. When profiling and risk assessment methods are also deployed in the security domain, for example, to track down potential fraudsters or criminals, the presumption of innocence is put under pressure. Whereas data is normally only collected *after* people are suspected, big data enables data and risk profiles to be prepared before there is an actual suspicion.

Conclusion

In this paper, we have described the societal and ethical issues emerging with the digitization of society on the basis of six dominant developing technologies: IoT, robotics, biometrics, persuasive technology, platforms, and augmented & virtual reality. Table 1 summarizes for each overarching theme the discussed societal and ethical issues evoked by these technologies. To underline the importance of these issues, we will briefly discuss the connection with important values set out in international treaties and fundamental rights.

Regulating big data and transparency of algorithms

The digitization of our material, biological and sociocultural world leads to an ever-expanding digital world of data. In that digital world, the data which is processed and analysed forms the basis for people as well as automated systems to make decisions that subsequently have an impact on the physical world. For all kinds of essential services and products, we make increasingly more use of digital technologies and we are becoming increasingly more dependent on digital systems: in healthcare, banking, media, education or the justice system. The digitization of society is entering a new phase, and has blurred the distinction between online and offline: we are *onlife*. Developments in the field of big data, smart algorithms based on artificial intelligence are indispensable elements of the technologies discussed above. These developments, for example, play a role with IoT devices that send information to the cloud (big data) and are at the same time steered by data and algorithms from the cloud to perform a specific action in the physical world. Big data and algorithms help to make decisions in the public and private sectors, from detecting fraud or the likelihood of reoffending, to medical diagnoses. In some areas, smart algorithms and intelligent systems are already taking

[24] http://www.autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-meer-privacywaarborgen-noodzakelijk-bij-toepassingen-big-data.

over decision-making from people, for example, with armed drones, or in smart cars. Technologies, embedded in advisory apps on our smartphone of in smart street lights, can be persuasive and may influence our behaviour and autonomy in subtle ways.

Due to digitization, there is now a lively trade in information. 'Big data' is sometimes referred to as 'new gold'. Data is valuable because it enables better decisions, for example, about which consumers should be shown which ad or which people should be investigated as potential fraudsters. We have already discussed various issues regarding privacy, and big data presents a specific challenge in this respect due to the re-use and potential combinations of different data sources. Combining and reusing big data seems to be at odds with the principle of purpose limitation, which is one of the pillars of data protection legislation. Various authors argue that legislation and supervision in the big data era should focus more on companies' responsibilities (accountability) and how data is used (Podesta et al. 2014; Cate et al. 2012). But opponents say that the principle of purpose limitation is an important mechanism to counteract unbridled collection and *data obesitas* (Hildebrandt 2015).

In addition, a significant characteristic of big data is that it is not clear beforehand which insights can be captured from the data. Researchers showed that on the basis of Facebook 'likes', it was possible to identify someone's sexual preference, religious and political orientation, personal characteristics and use of addictive substances (Kosinski et al. 2013). Authorities are also looking into big data's potential. One example is the Dutch anti-fraud system called System Risk Indication (SyRI) which encrypts, combines and analyses data about fines, debts, benefits, education and integration in a secure digital environment in order to search more effectively for people abusing benefits or surcharges. SyRI has been criticised by both the Data Protection Authority and the Senate because of the impact on privacy.

Data mining techniques (*data analytics*) and algorithms (combined with artificial intelligence, especially techniques such as *deep learning*) benefit immensely from the large amounts of data that have become available in recent years. The data forms coaching files for self-learning software: the more data the software gets, the smarter it becomes. Companies like Facebook and Google have facial recognition software that is improving quickly thanks to the many photos that users upload every day. Translation software is also improving because it can draw on a large number of officially translated documents from the United Nations and the European Commission (Mayer-Schonberger and Cukier 2013). In recent years, the discussions on monitoring the underlying algorithms in automated systems have come from different angles. The German Government recently released a position paper stating that online platforms—such as Google and Facebook—should provide more information about how their algorithms work, for example, when filtering news or search results.[25]

Public values

This study shows that the new wave of digitization is putting pressure on public values. ICT services and products are no longer gadgets: they are having a radical impact on our society. It is time to recognise the implications and to ensure that our public values and fundamental rights are safeguarded in the new digital era. The building blocks and the infrastructure for the new digital society are materializing now. The governance system to deal with the resulting social and ethical issues falls short in several dimensions, mainly because there is no clear understanding of the social and ethical issues implications of the digitization. Such an understanding is necessary so that these issues can be proactively addressed, that is, be anticipated, reflected upon, deliberated with the public and other stakeholders, and be responded to (Stahl et al. 2017; see also; Kizza 2013).

The supervision has been developed the most in the areas of privacy and data protection. For example, at European level, there has been an attempt to deal with big data issues by modifying the legislation. The new European Data Protection Regulation (EU 2016/679) building on the principles of the data protection directive (95/46/EC), adds a number of new obligations and responsibilities for data processors, and strengthens individual rights. This regulation shows that the topic of data is high on the agenda. However, there is also an ongoing debate about whether these legislative adjustments are adequate to deal with the inherent challenges of digitization. Particularly with regard to profiling, the legal framework only offers partial protection. For other ethical issues concerning digitization such as discrimination, autonomy, human dignity and unequal balance of power, the supervision is hardly organized. The most telling examples are the European Data Protection Supervisor initiatives (EDPS 2015, 2016), in particular to establish an ethics advisory group. Although social and ethical issues appear on the agenda, they are not being translated into policies that protect public values in practice. Supervisory bodies do not have enough insight in the emerging digitization issues. Likewise, civil society organizations and citizens are not sufficiently aware of the new digital developments, nor do they realise how they will be affected; the possibilities to defend themselves are too limited.

The need to focus on the effects of digitization is underlined by the fact that the central ethical themes relate to important values set down in international treaties and national constitutions. We can see issues such as privacy

[25] http://www.bmwi.de/DE/Presse/pressemitteilungen,did=764540.

and justice reflected in the right to respect for private life, the right to equal treatment and the right to a fair trial. Human dignity and safety are mentioned in international treaties such as the Charter of Fundamental Rights of the European Union (EU Charter) and the Universal Declaration of Human Rights (UDHR). Values such as autonomy, equal power relationships and control over technology are not explicitly named in the treaties but can be seen as part of or following from these fundamental and human rights. Digitization affects important public values.

The main task ahead of us is to effectively safeguard these widely acknowledged public values in our new digital society's everyday practices. Unless government, industry, civil society and members of the public act now, there is a risk that while we are trying to get to grips with the new digital world, the frameworks to protect public values are meanwhile losing their relevance.

References

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.

Arkin, R. (2010). The case for ethical autonomy in unmanned systems. *Journal of Military Ethics, 9*(4), 332–341.

Balkan, A. (2016). Digital being. *Arena Magazine, 143*(Aug/Sep),18–20.

Barbry, E. (2012). The internet of things, legal aspects: What will change (everything). *Communications & Strategies, 87*(3), 83–100.

Borenstein, J., & Pearson, Y. (2010). Robot caregivers: Harbingers of expanded freedom for all? *Ethics and Information Technology, 12*(3), 277–288.

Brinkman, B. (2014). Ethics and pervasive augmented reality: Some challenges and approaches. In K. D. Pimple (Ed.), Emerging pervasive information and communication technologies, pp. 149–175. Dordrecht: Springer.

Cate, F. H., Kuner, C., Millard, C., & Svantesson, D. J. B. (2012). The challenge of "big data" for data protection. *International Data Privacy Law, 2*(2), 47–49.

Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. *Washington Law Review, 89*, 1. https://ssrn.com/abstract=2376209.

Coeckelbergh, M. (2010). Health care, capabilities, and AI assistive technologies. *Ethical Theory and Moral Practice, 13*(2), 181–190.

Datta, A., Tschantz, M. C., & Datta, A. (2015). Automated experiments on ad privacy settings. A tale of opacity, choice, and discrimination. Proceedings on Privacy Enhancing Technologies (PoPETs 2015) (pp. 92–112). https://doi.org/10.1515/popets-2015-0007.

De Hert, P. J. A., & Sprokkereef, A. C. J. (2012). Second generation biometrics: The ethical, legal and social context. In E. Mordini & D. Tzovaras (Eds.), *Biometrics, Privacy and Agency* (pp. 81–101). Berlin: Springer.

Dotson, T. (2014). Authentic virtual others? The promise of post-modern technologies. *AI & Society, 29*(1), 11–21.

Dwoskin, E., & Rusli, E. M. (2015). The technology that unmasks your hidden emotions. Wall Street Journal (January 28). Accessed August 1, 2017, from https://wsj.com/articles/startups-see-your-face-unmask-your-emotions-1422472398#:bLk8dH_DkLSJvA.

EDPS (2015). Towards a new digital ethics: Data dignity and technology. Opinion 4/2015. Brussels: European Data Protection Supervisor.

EDPS (2016). Press Release: EDPS starts work on a new digital ethics. EDPS/2016/05. Accessed June 23, 2017, from https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2016/EDPS-2016-05-EDPS_Ethics_Advisory_Group_EN.pdf.

Floridi, L. (Ed.). (2015). *The onlife manifesto. Being human in a hyperconnected era*. Cham: Springer.

Fogg, B. J. (2002). *Persuasive technology: Using computers to change what we think and do*. Boston: Morgan Kaufmann.

Frenken, K., Meelen, T., Arets, M., & Van de Glind, P. (2015). Smarter regulation for the sharing economy. The Guardian (20 May). Accessed September 17, 2017, from https://www.theguardian.com/science/political-science/2015/may/20/smarter-regulation-for-the-sharing-economy.

Frenken, K., & Schor, J. (2017). Putting the sharing economy into perspective. *Environmental Innovation and Societal Transitions, 23*, 3–10.

Geser, H. (2010). Augmenting things, establishments and human beings. In: Sociology in Switzerland: Towards cybersociety and vireal social relations. Accessed June 13, 2017, from http://socio.ch/intcom/t_hgeser24.pdf.

Gibbs, S. (2015). Samsung's voice-recording smart TVs breach privacy law, campaigners claim. The Guardian (27 February). Accessed June 20, 2017, from http://theguardian.com/technology/2015/feb/27/samsung-voice-recording-smart-tv-breach-privacy-law-campaigners-claim.

Goodall, N. J. (2014). Ethical decision making during automated vehicle crashes. *Transportation Research Record: Journal of the Transportation Research Board, 2424*, 58–65.

Greenberg, A., & Zetter, K. (2015). How the internet of things got hacked. Wired (28 December). Accessed June 2, 2017, from http://wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked.

Hayles, N. K. (1999). *How we became posthuman: Virtual bodies in cybernetics, literature, and informatics*. Chicago: University of Chicago Press.

Heimo, O. I., Hakkala, A., & Kimppa, K. K. (2012). How to abuse biometric passport systems. *Journal of Information. Communication and Ethics in Society, 10*(2), 68–81.

Helbing, D., Frey, B. S., Gigerenzer, G., Hafen, E., Hagner, M., Hofstetter, et al. (2015). Digitale demokratie statt datendiktatur. Digital manifest. *Spektrum der Wissenschaft, 15*(12), 50–61.

Hern, A. (2014). Hacker fakes German minister's fingerprints using photos of her hands. The Guardian (30 December). Accessed May 15, 2017, from https://theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands.

Hildebrandt, M. (2012). The dawn of a critical transparency right for the profiling era. In J. Bus (Ed.), *Digital enlightenment yearbook 2012* (pp. 41–56). Amsterdam: IOS Press.

Hildebrandt, M. (2015). *Smart technologies and the end(s) of law: Novel entanglements of law and technology*. Cheltenham: Edward Elgar.

Hildebrandt, M. (2016). Law as information in the era of data-driven agency. *The Modern Law Review, 79*(1), 1–30.

Hilty, L. M. (2015). Ethical issues in ubiquitous computing: Three technology assessment studies revisited. In K. Kinder-Kurlanda & C. Ehrwein Nihan (Eds.), *Ubiquitous computing in the workplace. Advances in Intelligent Systems and Computing (volume 333)* (pp. 45–60). Cham: Springer.

Janssen, A., Kool, L., & Timmer, J. (2015). *Dicht op de huid. Gezichts- en emotieherkenning in Nederland*. The Hague: Rathenau Instituut.

Juul, N. C. (2013). Recommendation on the use of biometric technology. In P. Campisi (Ed.), *Security and privacy in biometrics* (pp. 415–433). London: Springer.

Kindt, E. J. (2013). *Privacy and data protection issues of biometric applications. A comparative legal analysis*. Dordrecht: Springer.

Kizza, J. M. (2013). *Ethical and social issues in the information age*. London: Springer.

Koops, E. J., & Prinsen, M. M. (2005). Glazen woning, transparant lichaam: Een toekomstblik op huisrecht en lichamelijke integriteit. *Nederlands Juristenblad, 80*(12), 624–630.

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, 110*(15), 5802–5805.

Kramer, A. D. I., Guillory, J. E., & Hancock, J. T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences, 111*(24), 8788–8790.

Kreijveld, M., Deuten, J., & Est, R. Van (Eds.). (2014). *De kracht van platformen. Nieuwe strategieën voor innoveren in een digitaliserende wereld*. The Hague/Deventer: Rathenau Instituut/ Vakmedianet.

Lee, P. (2012). Remoteness, risk and aircrew ethos. *Air Power Review, 15*(1), 1–19.

Louv, R. (2005). *Last child in the woods: Saving our children from nature-deficit disorder*. Chapel Hill, NC: Algonquin Books.

Maan, S., Merkus, B., Ham, J., & Midden, C. (2011). Making it not too obvious. The effect of ambient light feedback on space heating energy consumption. *Energy Efficiency, 4*(2), 175–183.

Madary, M., & Metzinger, T. K. (2016). Real virtuality: A code of ethical conduct. Recommendations for good scientific practice and the consumers of VR-technology. *Frontiers in Robotics and AI, 3*(3), https://doi.org/10.3389/frobt.2016.00003.

Mayer-Schonberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work and think*. Houghton: Mifflin Harcourt.

Meinrath, S. D., Losey, J., & Pickard, V. W. (2011). Digital feudalism: Enclosures and erasures from the digital rights management to the digital divide. *Commlaw Conspectus, 19*, 423–479.

Melson, G. F., Kahn, P. H., Beck, A., & Friedman, B. (2009). Robotic pets in human lives: Implications for the human-animal bond and for human relationships with personified technologies. *Journal of Social Issues, 65*(3), 545–569.

Mordini, E., Tzovaras, D., & Ashton, H. (2012). Introduction. In E. Mordini & D. Tzovaras (Eds.), *Second generation biometrics: The ethical, legal and social context. The International Library of Ethics, Law and Technology (volume 11)* (pp. 1–19). Dordrecht: Springer.

Morozov, E. (2014). The rise of data and the death of politics. The Guardian (20 July). Accessed May 15, 2017, from https://www.theguardian.com/technology/2014/jul/20/rise-of-data-death-of-politics-evgeny-morozov-algorithmic-regulation.

O'Brolchain, F., Jacquemard, T., Monaghan, D., O'Connor, N., Novitzky, P., & Gordijn, B. (2016). The convergence of virtual reality and social networks: Threats to privacy and autonomy. *Science and Engineering Ethics, 22*(1), 1–29.

Pariser, E. (2011). *The filter bubble: What the Internet is hiding from you*. New York: Penguin Press.

Parker, G., & Van Alstyne, M. W. (2017). Innovation, openness, and platform control. *Management Science*. https://doi.org/10.1287/mnsc.2017.2757.

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Cambridge, MA: Harvard University Press.

Peck, D. (2013). They're watching you at work. The Atlantic. December 2013 issue. Accessed March 17, 2017, from http://www.theatlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681/.

Peppet, S. R. (2014). Regulating the internet of things: First steps towards managing discrimination, privacy, security and consent. *Texas Law Review, 93*, 85–176.

Pereira, A. G., Benessia, A., & Curvelo, P. (2013). *Agency in the internet of things*. Luxembourg: Publications Office of the European Union.

Podesta, J., Pritzker, P., Moniz, E., Holdren, J., & Zients, J. (2014). *Big Data: Seizing opportunities, preserving values*. Washington: Executive Office of the President.

Rani, A. (2013). The Japanese men who prefer virtual girlfriends to sex. BBC, 24-10-2013. Accessed October 14, 2017, from http://www.bbc.com/news/magazine-24614830. .

Renaud, K., Hoskins, A., & Von Solms, R. (2015). Biometric identification: Are we ethically ready? Information Security for South Africa (ISSA2015). Johannesburg (12–13 August). Accessed August 1, 2017, from http://ieeexplore.ieee.org/document/7335051/?reload=true.

Rogers, B. (2015). The social costs of Uber. *The University of Chicago Law Review Dialogue, 82*, 85–102.

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. *Computer Networks, 57*(10), 2266–2279.

Royakkers, L. M. M., & Van Est, Q. (2010). The cubicle warrior: The marionette of the digitalized warfare. *Ethics and Information Technology, 12*(3), 289–296.

Sandhya, M., & Prasad, M. V. N. K. (2017). Biometric template protection: A systematic literature review of approaches and modalities. In R. Jiang et al. (Eds.), *Biometric security and privacy. Opportunities & challenges in the big data era* (pp. 323–370). Cham: Springer.

Scholz, L. H. (2017). Algorithmic contracts. Stanford Technology Law Review.

Scholz, T. (2016). *Platform cooperativism. Challenging the corporate sharing economy*. New York: Rosa Luxemburg Stiftung.

Seddon, R. F. J. (2013). Getting 'virtual' wrongs right. *Ethics and Information Technology, 15*(1), 1–11.

Sharkey, A. (2014). Robots and human dignity: A consideration of the effects of robot care on the dignity of older people. *Ethics and Information Technology, 16*(1), 63–75.

Sharkey, N. (2010). Saying 'no!' to lethal autonomous targeting. *Journal of Military Ethics, 9*(4), 369–383.

Smids, J. (2012). The voluntariness of persuasive technology. In M. Bang & E. L. Ragnemalm (Eds.), *Persuasive technology. Design for health and safety. PERSUASIVE 2012. Lecture Notes in Computer Science* (Vol. 7284, pp. 123–132). Berlin: Springer.

Spahn, A. (2012). And lead us (not) into persuasion…? Persuasive technology and the ethics of communication. *Science and Engineering Ethics, 18*(4), 1–18.

Spahn, A. (2013). Ideas in motion. Moralizing mobility? Persuasive technologies and the ethics of mobility. *Transfer, 3*(2), 108–115.

Stahl, B. C., Timmermans, J., & Flick, C. (2017). Ethics of emerging information and communication technologies. On the implementation of responsible research and innovation. *Science and Public Policy, 44*(3), 369–381.

Stone, B. (2009). Amazon erases Orwell books from kindle. New York Times (17 July). Accessed September 4, 2017, from http://

www.nytimes.com/2009/07/18/technology/companies/18amazon.html?_r=1.

Sullins, J. P. (2012). Robots, love and sex: The ethics of building love machines. *Affective Computing, 3*(4), 398–409.

Sutrop (2010). Ethical issues in governing biometric technologies. In A. Kumar & D. Zhang (Eds.), *Ethics and policy of biometrics* (Lecture Notes in Computer Science, Volume 6005, pp. 102–114). Heidelberg: Springer.

Sutrop, M., & Laas-Mikko, K. (2012). From identity verification to behavior prediction: Ethical implications of second generation biometrics. *Review of Policy Research, 29*(1), 21–36.

Timmer, J., Kool, L., & van Est, R. (2015). Ethical issues in emerging applications of persuasive technologies. In T. MacTavish & S. Basapur (Eds.), *Persuasive Technology. PERSUASIVE 2015. Lecture Notes in Computer Science* (Vol. 9072, pp. 196–201). Cham: Springer.

Turilli, M., & Floridi, L. (2009). The ethics of information transparency. *Ethics and Information Technology, 11*(2), 105–112.

Turkle, S. (2011). *Alone together. Why we expect more from technology and less from each other*. New York: Basic Books.

Tzanou, M. (2017). *Fundamental right to data protection: Normative value in the context of counter-terrorism surveillance*. Oxford: Hart.

Van der Ploeg, I. (2007). Genetics, biometrics and the informatization of the body. *Ann Ist Super Sanita, 43*(1), 44–50.

Van Est, R. (2014). *Intimate technology: The battle for our body and behaviour*. The Hague: Rathenau Instituut.

Van Est, R., & Kool, L. (2015). *Working on the robot society. Visions and insights from science about the relation technology and employment*. The Hague: Rathenau Instituut.

Van Wynsberghe, A. (2015). *Robots in healthcare: Design, use and implementation*. Farnham: Ashgate.

Walker, S. (2016). Face recognition app taking Russia by storm may bring end to public anonymity. The Guardian (17 May). Accessed May 15, 2017, from https://theguardian.com/technology/2016/may/17/findface-face-recognition-app-end-public-anonymity-vkontakte.

Walsh, K. (2016). Nest reminds customers that ownership isn't what it used to be. EFF (5 April). Accessed May 27, 2017, from https://www.eff.org/deeplinks/2016/04/nest-reminds-customers-ownership-isnt-what-it-used-be.

Wolf, M. J., Grodzinsky, F., & Miller, K. (2015). Augmented reality all around us: Power and perception at a crossroads. *SIGCAS Computers & Society, 45*(3), 126–131.

Zarksy (2013). Transparent predictions, SSRN. Accessed January 4, 2018, from http://papers.ssrn.com/sol3/ papers.cfm?abstract_id = 2324240.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30*(1), 75–89.