RISE OF THE SMART MACHINES

A socio-legal analysis of the concept of privacy beyond the screen in the home, its problems, and the significance of the protection of different objects of privacy in the smart world

Lisa van Dongen

INTRODUCTION

Privacy has gained more attention over the years in both politics and legal scholarship due to rapid technological advancements such as digital identification methods, smart objects and genetic testing, along with the widespread adoption of information and communication technologies and the development of the 'Internet of Things'. The Internet has become a prime platform for communication and consuming, not just via our laptop, but also via *inter alia* our smart thermostat that is linked to other technological objects inside the home and to an external service provider. Even governmental services such as tax returns have gone digital and require the individual to go online. Consequently, a lot more information is shared than the average individual perhaps is willing to share, and most likely more than the average individual is aware of (Mik, 2016). The European Union has attempted to legally mitigate the threats to privacy of the individual posed by these developments via providing for data protection by inter alia the adoption of Regulation (EU) 2016/697 on the processing and free movement of personal data. The attention paid to data protection, and the addressing of some of the problems arising in this area is without a doubt a very positive development since it shows that a problem is recognised, as well as the need to address it. However, data protection can only protect the informational representation of aspects of the personal life, and is therefore insufficient to address the concept of privacy as a whole, as will be argued here. By only focusing on data protection, the other objects of privacy are overlooked, as well as their harms. This is problematic since we are moving away from screen-based data capturing and processing to a smart world filled with intelligent and smart objects without a screen in which the line between 'online' and 'offline' has become blurred (Mattern, 2002 & 2003 as cited in Röcker, 2010). Consequently, it has become necessary to rethink our current approach to privacy protection. Unfortunately, privacy and related socio-ethical problems and tensions in private spaces that may arise in the interaction of humans with technological objects embedded with computation without a 'screen' have not received much attention. Privacy beyond the screen has been mentioned in several pieces of literature and by European agencies (see Eskens, Timmer, Kool & Van Est, 2016; European Data Protection Supervisor, 2015), and it is identified as a potential problem in today's approach to privacy, yet there have been no real attempts to set the perimeters of this concept. This has resulted in the concept of privacy beyond the screen in (semi-)private spaces to remain somewhat vague and challenging to address effectively. This paper will attempt to give this concept more body in order to get a grip on some of the privacy-related problems with this concept, and thus attempt to answer the questions:

What are the relevant features of technological objects under the concept of privacy beyond the screen? What are some of the (possible) legal, ethical and sociological privacy-related problems with regard to this concept in respect of the home?

In answering this question, this paper aims to make it evident that the focus on data protection in combination with the quick progression in technology proves problematic for privacy 'beyond the screen' in private spaces. The aim here is not to introduce solutions to the identified problems, but to provide some food for thought and add fuel to the discussion on the importance of privacy beyond the digital representation of aspects of the personal life today. The starting point in this paper is that it is not just informational privacy that is at stake. Therefore, this paper will start off with a general analysis of the concept of privacy 'beyond the screen' in the home via the establishment of categories, while making an assessment of possible relevant factors for those categories as well as for the autonomy and 'choice' of the individual in Part I. In addition, special attention will also be paid to the importance of trust in technology as an influence on how the individual can operate a technological object from a privacy perspective, but also in respect of potential impediments for trust. In Part II, an analysis will first be made of the objective of data protection, followed by a brief substantiation of other, 'physical' objects of privacy. The objects of privacy will then be connected to specific cases for which the research conducted in Koops et al. (2016) will be guiding. Although some of their approaches or findings may be deemed controversial or limited by some with regard to their ideal types, the analysis on the objects of privacy found in this research will, nevertheless, lend themselves for analyses conducted in this paper since they are all widely recognised in some form, both directly and indirectly, in law and legal scholarship. The reason the typology of privacy in this paper is chosen is the extensiveness of the analysis of both law and legal scholarship in a wide range of countries from different legal systems and histories on which their typology is based (see Koops et al., 2016 for their methodology).

Furthermore, some of the privacy-related problems in these specific cases will be reflected upon from both an ethical and sociological perspective. The focus of this paper will be on objects situated inside the home, and will therefore leave sensors and other (invisible) sources of information gathering objects outside the home out of the picture. Although the latter category is certainly not less relevant for privacy beyond the screen (see Lahlou, Langheinrich & Röcker, 2005), it would, among other things, require additional analysis of privacy in public and semi-public spaces, which cannot be achieved in this limited sized contribution. Furthermore, with the significant amount of literature already dedicated to surveillance and privacy with regard to public and semi-public spaces, the emphasis on the home as the (legal) background is deemed more beneficial for the discussion on privacy 'beyond the screen' today. Moreover, this limited scope enables the analysis to be more cohesive and imaging due the support of specific examples within the private sphere.

PART I: GENERAL ANALYSIS OF 'BEYOND THE SCREEN'

I.I New challenges posed by an old problem

With the coming into being of the Internet people already have experience with the information flow and its increasing speed and accessibility, so the availability of information is not something new (Röcker,

2010). However, more objects make it into our homes that are not only embedded with computation, but are also "subject to control by servers external to the home, or … mobile technologies that regularly leave the home's perimeter and [can] interact with other networks" (Denning, Kohno & Levy, 2013, p. 94). Such technological objects are capable of reacting to changes "within the environment with respect to the user and other devices and services" enabled by the interaction of the object with both the user and other smart objects (Davy, 2003, p. 6; Poslad, 2009). This makes it more difficult, if not practically impossible, for human actors to control or 'manage' this information flow (Bohn, Coroamă, Langheinrich, Mattern & Rohs, 2004; Röcker, 2010), even more so in the absence of a screen.

So, the problem may be old, but its effect is increasingly invasive and of new proportions. Admittedly, this information flow is essential for the usage of smart objects since they depend on information input to best serve us and to be able to evolve to remain effective (Lahlou, Langheinrich & Röcker, 2005; Poslad, 2009), yet the danger arises that, as Dobbins nicely put it, "[t]he integration of these high tech features creates avenues for unsolicited data collection", both quantitatively and qualitatively (2015, p. 1; Manta & Olson, 2015), and "potential computer security attacks against in-home technologies" (Denning, Kohno & Levy, 2013, p. 94). The interaction of smart objects with environments has blurred the lines between offline and online in the sense that the collecting by a single technological object is no longer limited to only the 'online use' (Mattern, 2002 & 2003 as cited in Röcker, 2010). This effect is increased even more by the way these objects are designed, meaning that these objects may often not be perceived as computers at all, as is the case in particular with smart or intelligent technology without 'screens'. According to Röcker, "[the] vision of Ubiquitous Computing implies, that computers are integrated into the physical environment, and hence are effectively invisible to the user, rather than being distinct objects on the desktop" (2010, p. 62). Another issue that has gained in prominence, also caused by the continuing increase of "the number of services available to users[, is the] … need to maintain the user's identity in a secured, trusted manner" (Hsiung, Scheurich & Ferrante, 2001, p. 45). People rely on the 'promised' anonymity or pseudonyms for most of the information that they essentially provide themselves to external actors by using smart technology, but in reality, this might not really provide protection due to the more detailed profiles and the increasing sophistication of algorithms (Hsiung, Scheurich & Ferrante, 2001). Pseudonymised/anonymised or not, these profiles may contain enough information to be retrospectively linked to individuals (Mattern, 2005 as cited in Röcker, 2010). A human operator can 'erase' personal information from some personal devices such as an iPad, and in some jurisdictions it is possible for individuals to request companies to delete certain personal information, but that does not mean that the information is really gone. For other devices, this type of information management is difficult or even impossible, due to the absence of a screen and/or privacy settings.

For law and society, the novel technologies and the spreading of adoption of ICTs by all sorts of actors in society is not just about replacing old technology with updated versions and newer, more sophisticated inventions (Koops, 2011); these new or increasingly advancing developments cannot just bring on significant changes in the socio-political order due to new or more invasive surveillance and data retrieval technologies (see Milaj, 2015), they can also cause a rapid decrease of individuals' trust in their environment (Bohn et al. 2004 & 2005 as cited in Röcker, 2010). Trust is a subjective belief that can be observed from different perspectives and in different contexts, and its influence depends on different

actors, interactions and environments (Kim, Song, Braynov & Rao, 2005). Arguably, from the angle of trust in technology, the relationship between consumers and businesses should not be ignored in the case of smart objects since the businesses are on the other end of the processes, but it revolves more clearly around the confidence of consumers in the processes itself when discussing objects capable of functioning autonomously (Kim, Song, Braynov & Rao, 2005; Mik, 2016). When consumer confidence is low or decreases, this will also affect the rise and development of such technologies (Röcker, 2010; Kim, Song, Braynov & Rao, 2005; Hsiung, Scheurich & Ferrante, 2001). Moreover, the more complicated and sophisticated technology becomes, the more distance will come between the intelligent and smart objects and the human operators on the consumer end. For instance, the general consumer may not be able to predict the behaviour of such an object situated in his or her own home (Röcker, 2010; Mik, 2016), arguably the most prominent form of 'private space', or will find him or herself unable to manage and/or control what the technology does, which will affect how the technology is perceived and used. This is particularly apparent when it comes to devices that do not come with a screen, or when it does have a screen but nevertheless does not provide the human actor with the possibility to 'control, manage or monitor' the functioning of the object and/ or information flow (Lahlou, Langheinrich & Röcker, 2005; Eskens, Timmer, Kool & Van Est, 2016; European Data Protection Supervisor, 2015). Individuals would not be able to verify *inter alia* whether the technology is functioning properly, or when it is being misused by externalities (e.g. manufacturer, the government), and this loss of control and the dependency that mankind creates for itself could ultimately lead to "users … [becoming] mistrustful and … [seeing] the objects in a negative light" (Von Locquenghien, 2006 as cited in Röcker, 2010, p. 64). The increasing amount of intelligent and smart technology entering our homes thus requires a "sense of the 'loyalty' of objects inhabiting the environment" (Bohn, Coroama, Langheinrich, Mattern & Rohs, 2003 as cited in Röcker, 2010, p. 64) for the 'Internet of Things' to become successful. In other words: trust is imperative for the increasing autonomy of our surroundings.

The lack of trust can thus limit the growth and usage of technology (Kim, Song, Braynov & Rao, 2005; Hsiung, Scheurich & Ferrante, 2001), but it will in all likelihood eventually not stop the intelligent and smart technology from increasing its prominence. It has been argued by some scholars that generally the rejection of certain technology does not last long, and that regardless of the previous reservations, "people tend to forget quickly what things used to be like" (see Pearson, 2001, as cited in Röcker, 2010, p. 65; Mattern, 2003 as cited in Röcker, 2010). Herein lies the danger that bring us full circle: it is an old problem of new proportions that threatens trust of individuals in their direct surroundings, their autonomy, and, most importantly for this paper, privacy. Privacy beyond the screen is part of the new challenges of this old problem. If we look at privacy beyond the screen from a consumer's perspective this may even be one of the biggest issues in the rise of the 'Internet of Things', given that it has only received some attention, while smart technology without screens is entering our homes in increasing numbers. A problem with concepts that have not been subjected to extensive analyses is that they remain somewhat vague, and therefore they run the risk of being underestimated, and ultimately of remaining (partially) unaddressed. In the field of data protection, there are some instruments in place (and more are on their way) that affect and mitigate some of the negative effects for privacy that may arise, but as argued shortly in the introduction: data protection does not equal privacy protection. Information privacy touches upon and overlaps with all other objects and types of privacy since it entails the protection of

information about the objects of privacy "that can be directly "watched" or intruded upon" (Koops et al., 2016, p. 58; Cohen, 2008), but it is an independent concept of which a part has little to do with privacy (Cuijpers, Leenes, Olislaegers & Stuurman, 2011). They are, therefore, distinct but interdependent (Cohen, 2008). This means that data protection alone will not be sufficient to protect privacy in the near future, and may even compromise the protection of objects of privacy since data protection measures may only cover them partially, or may even be in conflict with their objective. Before case analyses can be conducted in this respect in Part II to substantiate this claim, it is first imperative that the concept of 'privacy beyond the screen' will be analysed to get rid of some of the 'fog' around it.

1.3 The categories and general issues

First, to get a better understanding of the privacy-related problems examined with regard to the concept of privacy beyond the screen, the distinction is made between the capabilities of technological objects inside the home without interference from external actors outside the home such as the manufacturer (digitisation of the home) from the ability to access the information by external actors (Koops, Van Schooten & Prinsen, 2004). This can be seen as a two-tiered information flow that entails the collecting, processing, storing, connecting and transmitting of information by the technological objects inside the home when used by human actors in the first tier (Kortuem, Kawsar, Sundramoorthy & Fitton, 2010), likely followed by the collecting, processing and storing of such information situated on the technological objects by external receivers (via cloud, company database, etc.) in the second tier (Denning, Kohno & Levy, 2013; Röcker, 2010; Lahlou, Langheinrich, & Röcker, 2005).

Second, in order to give the concept of privacy 'beyond the screen' more body the concept must be broken down in categories, which also allows for a better understanding of the problems that come with it. To clarify these categories, examples will be used that will be addressed in more detail in Part II, of which some may not seem problematic yet, or so far unable to perform the two-tiered information flow as proposed here. However, with the rapidly advancing technological developments of the recent years in mind, held together with the push from the industry and even governments towards an 'Internet of Things' (see Shin, 2014) and the increase of smart objects entering our lives and homes (see Helal, et al, 2015; Kortuem, Kawsar, Sundramoorthy & Fitton, 2010), these examples are a great way to illustrate just how much technology can change our lives and homes, and thereby how real the threat that accompanies these developments is or can become when it is not addressed properly (Bohn et al, 2004; European Parliament, 2015; Dobbins, 2015). According to Langheinrich and Mattern (2002) "technological developments [so far] never intended to change the world or society, but rather did so as a side effect" (as cited in Röcker, 2010, p. 61). Bohn et al. argue in addition that "in contrast, the vision of Ubiquitous Computing explicitly aims at transforming the world" (2004 & 2005 as cited in Röcker, 2010, p. 61) "by providing technology, that will accompany us throughout our whole lives, day in and day out" (Langheinrich & Mattern, 2002 as cited in Röcker, 2010, p. 61).

For privacy 'beyond the screen', the obvious distinction to be made first from a privacy perspective is between technology with screen and that without. However, when looking for examples of the latter category, it seems that this distinction may not be as obvious to determine in practice as, for example, both Hello Barbie and lighting systems could qualify in this category. Both examples will also be part of the case assessments in Part II. The first example connects, collects and transmits information

on its own when it is used without assistance from or control by other devices, while the second example could (but not necessarily) be solely controlled via another device operated by the same human operator, a general platform of some sort from which all devices can be controlled. This general control centre could be a central home system for multiple devices, but there is also the trend of objects being controlled via applications on more personal, portable devices such as iPads and smartphones. Even in the absence of a clear definition for the category of 'beyond the screen' 'Hello Barbie' will probably meet little resistance when qualified as 'without screen'. However, the second example could have some sort of screen through which it is operated and controlled via these other 'control devices'. It is plausible that (now or in the near future) technological objects such as lighting systems will come to depend solely on the second device for the human actor to be able to (de)activate and operate it due to the absence of simple switches for the object, itself, or perhaps completely on sensors alone. As a matter of fact, there are already 'smart' spaces and buildings,[1] and lighting systems in a lot of office buildings that work via sensors, only. The question that follows is then to which extent the collecting, processing and possible storing of the collected information in both tiers can be controlled via the 'control device' for technology as the second example to still qualify as technology 'without a screen'. This problem can also be reversed: what does 'screen' really mean with regard to privacy? A workable distinction that can be made here is between objects with screens that allow for privacy settings to be adjusted by the human operator, in which context the individual could be deemed 'in control' (to a certain extent) such as an iPad or laptop, and those without adjustable privacy settings, thereby not allowing for control by the individual. An example of the latter context would be a smart thermostat such as 'Toon', which does have a screen, but the screen on that type of technology does (so far/generally) not allow for such personal settings.

To clarify, 'control' here does not entail the choice of the individual 'to use or not to use'. Control in this context refers to the possibility for the individual to exercise any control in using the object with regard to the functioning and information flow via some kind of adjustable privacy settings. Interesting and relevant to mention here is that even if the technological object provides for 'control by the individual' in this sense, it is still questionable whether the individual is likely to exercise it in practice due to *inter alia* the design of the object.[2] Such externalities do cast a shadow on the feasibility of 'choice' to be autonomous, for it is likely to interfere with the true needs and wants of the individual in question to act on, and the ability and likelihood that the individual will actually exercise control in this perspective (Mik, 2016; Harris, 2016). Notwithstanding the fact that autonomy is a difficult concept to grasp, useful approaches to this concept for this analysis are *inter alia* the negative perspective from which Brownsword defines autonomy as the lack of externalities to influence or limit an individual's decision making or actions (2011; Mik, 2016), and the often made connection of autonomy to "the ability to make choices and further one's interests" (Radin, 2000 and Calo, 2014 as cited in Mik, 2015, p. 9). The context is unlikely to ever be free of externalities influencing 'choice', but as Baldwin proposed, it

[1] "A Smart Space is a physical space rich in devices and software services that is capable of interacting with people, the physical environment and external networked services" (Davy, 2003, see also MZones, 2003).

[2] A very well-known theory of note to mention here would be that technology is 'scripted' in the sense that the human operator is to follow the script embedded in the technology, which thereby constrains the actions of the human operator in the usage (Akrich, 1992 as cited in Howcroft, Mitev & Wilson, 2004). A valid argument in this respect would be that "control requires competence" (Mik, 2016, p. 32).

matters whether the externalities can be identified and managed to a degree that preserves the individual's autonomy (2014 as cited in Mik, 2016). It seems highly probable that technology that transforms to better serve the individual based on the collected and analysed information on this person would be found 'guilty as charged'. Consequently, the concept of individual choice in the manner of usage and information flow loses some of its shine in practice, and will come down to a lot of case-by-case assessments. Nevertheless, for the purpose of developing a rudimentary definition and/or to distinguish workable elements for privacy 'beyond the screen', the distinction in technological objects between those with screens and those without, and between those with adjustable privacy settings and technological objects without such adjustable settings is imperative, since no problem can be tackled without the identification of the most prudent elements to look for in an assessment.

The category of 'no adjustable privacy settings' can be further divided into technological objects with monitoring capabilities and those that do not possess that quality. This is where it gets really interesting, since monitoring capabilities can be explained in two very different ways. First, from the consumer's perspective it can be explained as the (in)ability for the individual to monitor him or herself what happens to information in one or both tiers, which would provide the individual with a better and possibly more comprehensive insight to the 'cost' of using the technological object in question. The smart thermostat 'Toon' does not provide for that ability, but a possible example that does could be 'apps' for smart devices. Apps can and should be included here instead of under the category of 'without a screen', because they do not merely provide for the possibility to be controlled or operated via another device that functions as the 'control device' as is the case with the lighting systems; they are specifically designed to be used on certain technological objects with screen, and are completely depended on those objects. Moreover, a lot of apps today are meant to enable the human actor to control or operate other smart objects remotely via their 'home smart device', which is contrary to the example of lighting systems under the category of 'without screen'. In addition, when an individual wants to download and install these applications, generally he or she has to go through the list of other applications and additional sources of information on the personal device that the provider of this application will gain access to when the individual agrees with the provider's terms. The individual does not really have a choice if he/she wants to use this application, nor will any control be possible in retrospect when the general consent is given prior to usage, but the individual can take notice of what kind of information may be shared with this application and its provider. This means that in theory, the individual would be able to monitor the collecting and transmitting of the data conducted by the app, and therefore make the choice on whether to use the object. However, in practice this 'choice' does not allow for much autonomous decision making by the individual due to all kinds of societal and practical factors relevant to the (non)usage of the object (see Bohn et al, 2004; Van Wynsberghe, 2012; Harris, 2016).[3]

[3] As aforementioned, the strength and feasibility of autonomous decision-making of the individual can be questioned with regard to the control exercised by the individual, but this is also true for the mere choice of 'to use or not to use'. An interesting comment in this respect is made by Shin (2014): "It is obvious that connected devices are possible, but we are not exactly sure why we need them." In principle, the aim of developing technology is that it will become necessary and adds to the quality of life (Van Wynsberghe, 2012; Shin, 2014).

Second, from the perspective of the industry, monitoring capabilities can be divided into what they (can) do with the acquired information, and to what influence the external actor(s) has (if at all) on what happens in the first tier. Especially the latter brings on a lot of questions: can it turn itself on and monitor on its 'own initiative'? What is the relevance and what are the consequences for privacy when it is not the company behind the product that provides for the behaviour after it has been purchased, in the sense that both the consumer and business can only monitor the information (and in the latter's position possibly process and store this information) on which basis the object is acting? Smart objects are already capable of interpreting and performing "intelligent operations on [their] own [and] behave with respect to its functionality and its relevant surrounding environment" (Davy, 2003, p. 6; Kortuem, Kawsar, Sundramoorthy & Fitton, 2010; Streitz et al, 2005), so aside from liability issues and risk assessments, these questions are very relevant to privacy-related issues when more and more of such smart objects enter the home, but also to ethical and sociological issues that arise in the scenario that the external actor(s) can only account for the second tier information flow, and not for how the technological object acquires information, and what it does with it. This is all the more pressing if there are several technological objects with two-tiered capabilities from a different nature, both in task and position in the house (e.g. the connection and sharing of information between an object situated in the bathroom or a bedroom with an object in the living room), that share information while they have different external actors outside of the home to provide with the information they acquire, as well.

According to Denning, Kohno & Levy, the home, with its private and semi-private spaces and "[i]nterpersonal dynamics [of residents with] varying levels of security expertise, and different social and technical preferences all contribute to complicating the home technology security landscape" (2013, p. 96). This is also true in the context of privacy when all these objects are interconnected. When one would apply this scenario to the smart coffee machine, it could refuse to give coffee to you because you have already consumed more than usual, or perhaps because it can connect to your smart phone via which your GP has told you to slow down on your caffeine consumption. This might already be a scary thought due to the autonomy with which the smart object operates, thereby effectively taking away the ability of the human operator to choose for him or herself (see Mik, 2016) completely, but an accompanying issue would be the fact that it could also refuse to accommodate fellow residents. While this is already problematic, this is (just) about coffee. What happens when the refrigerator denies other residents access to food inside the fridge? This could be prevented if the smart coffee machine (or refrigerator) were able to identify the human operator directly (not based on previous analyses). However, to have this kind of technology embedded in every technological object in the house while they are working autonomously to such an extent may be deemed very undesirable under the existing legal and ethical framework on privacy, especially when it involves a family with children (Dobbins, 2015). In the case of multiple residents, another relevant question to as is: whose directions should be granted the most weight? How is this determined, and by who, or perhaps by what?

Also relevant here is the inability for the external actor to only allow for certain information necessary for the functioning of the technological object to be collected instead of unsolicited and unlimited 'mining' by the object, itself, but one could also argue that this inability would also prevent the external actor from 'mining', himself. Even though the latter is a very compelling argument that should not be ignored, especially when one takes the security issues in mind that also accompany the

developments in smart technology (Denning, Kohno & Levy, 2013), the idea of having a human operator that is able to intervene and can be held responsible instead of an object in your house as the sole operator behind the collecting of information might still be preferable due to some of the persevering issues in the current state of implementing ethics into technology when it involves such a privacy-sensitive space as the home (Van Wynsberghe, 2012). The home, particularly, is arguably the centre of our privacy, "because of the role that private space plays in preventing access to intimate activities" (Koops et al., 2016). If the technological objects inside our home affect the protection offered by the home from the inside out, it is time to take another look at the objects of privacy protection, and in particular at the objective of data protection. The latter will be assessed in Part II to see whether it is able to weather today's and tomorrow's challenges with regard to privacy beyond the screen, with the objective to establish the diversity of the problem in respect of privacy protection in an increasingly smarter home. This will pave the way for more specific case assessments in which other objects of privacy can be linked to certain technological objects alongside informational privacy.

PART II: SPECTRUM OF 'BEYOND THE SCREEN'

II.1 The objects of privacy

To illustrate the concept of privacy beyond the screen and the related problems, while demonstrating the importance of a broader notion of privacy than just informational privacy, a further analysis of the examples of the 'no screen' categories will be conducted, along with a more general analysis of the 'no monitoring capabilities' category. For this elaborated comparison, the scene must first be set to allow for a more comprehensive case-by-case analysis in respect of some of the impediments that can be observed, which will be done by means of an analysis of the objective pursued by data protection in the light of the European Convention on Human Rights (hereinafter: ECHR) and law of the European Union, and of other objects of privacy protection relevant for the case assessments. Apart from data protection, there are five main objects of privacy relevant to the case assessments conducted below: privacy of the home, property, and of person (e.g. thought, autonomy, bodily integrity). In order to further demonstrate how apparent and pressing this problem is, some of the relevant related problems for privacy will be further outlined via the case assessments on some of the smart objects relevant for the category of 'privacy beyond the screen' that are mostly situated inside the home, by tying them to these objects of privacy. The case assessments will allow for a more comprehensive illustration of some of the ethical and sociological problems that arise in this area, in addition to the more general analysis on some of these issues already addressed above in Part I.I and I.2.

Finally, it must be pointed out that attention will not be paid to the positive or negative nature of the protection provided for in the legal instruments mentioned above, nor to the distinction between the freedoms and rights, simply because that is not necessary to determine the objects of privacy, but mostly because a more general analysis is more beneficial to the objective this paper aims to achieve.

II.1.1 Data protection

In Europe, there are two clearly distinguishable legal systems (apart from the European states) in which data protection has been regulated: the Council of Europe and the European Union.

Under the Council of Europe, data protection or information privacy is part of the general "Right to respect for private and family life".[4] A right to data protection has been recognised and developed via the case law of the Strasbourg Court, as well as the horizontal effect of this Article, which has become widely acknowledged, even though it was initially meant to protect the individual against the state (Cuijpers, Leenes, Olislaegers & Stuurman, 2011; Koops, 2011). The Council of Europe, as a leading human rights organisation, aims:

"[To] secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")."[5]

In the legal framework of the Council of Europe, data protection applies to the automatic processing of personal data, which includes *inter alia* the storage, retrieval, and conducting of logical and/or arithmetical operations on any type of data capable of identifying an individual. Arguably, some of the functions of intelligent and smart objects would seem to fall within this scope, as well as the activities performed by the external actors on the other end of the processes.

In the legal framework of the European Union on data protection, the objective is the protection of "fundamental rights and freedoms of natural persons, and in particular their right to privacy".[6][7] The EU aims "to ensure free movement of personal data while guaranteeing a high level of protection for the rights and interests of the individuals to whom such data relate", as argued by the Court of Justice of the European Union in *Kingdom of Sweden vs Bodil Lindqvist* (2003, para. 96) in its preliminary ruling. In the European legal framework on personal information both individuals and the private industry are addressed, alongside the government of the Member States, so it seems that it provides for horizontal effect to some extent, as well (Cuijpers, Leenes, Olislaegers & Stuurman, 2011). In this legal framework, guidance is provided on what types of data are included in the definition of personal data by which natural persons can be identified, and any form of operation of such data should comply with the rules and principles of EU legal instruments on data protection.[8]

---

[4] Article 8 ECHR.

[5] Article 1 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, CETS No. 108, 1981. Convention 108 is a legally binding, international instrument that applies to the automatic processing of personal data by both private and public actors (European Union Agency for Fundamental Rights, 2014).

[6] Article 1(1) Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. However, this Directive will soon be replaced by a newly adopted regulation that will apply from 25 May 2018, namely Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ L 119, 4.5.2016, p. 1–88). "The Regulation is an essential step to strengthen citizens' fundamental rights in the digital age and facilitate business by simplifying rules for companies in the Digital Single Market." (European Commission, 2016).

[7] The right to data protection is laid down in Article 8 of the EU Charter of Fundamental Rights (hereinafter: EU Charter).

[8] Article 2(a) and (b) Directive 95/46/EC and Articles 4(1), (2) and 5 Regulation (EU) No. 2016/679;

It is clear from these legal frameworks that data protection also contains a part that has nothing to do with privacy, because not all data is of a personal nature, nor does "all personal data [relate] to the personal life" (Koops et al., 2016, p. 45). This means that if the main focus is on data protection instead of on privacy, other objects of privacy and non-identifying, privacy-sensitive information about those objects are excluded from the scope of data protection. The protection of other objects of privacy in addition to data protection is thus imperative, as will be demonstrated by the case assessments.

II.1.2 Privacy of the home

In particular the home is interesting when considering the 'Internet of Things' with all the type of smart objects making their way into our homes, and the reasonable expectation of privacy one may have for the combination of a specific place, situation, and the type of activity commenced/service of the object used.

Privacy of the home is very broadly defined in the legal framework of the Council of Europe and in the case law of the Strasbourg court:[9] The home is "where one lives on a settled basis", which basically includes all living spaces except for "temporary long-term accommodations" such as holiday homes (Kilkelly, 2001, p. 19). In *Niemietz vs. Germany* (1992), the Strasbourg Court stated that even the professional life and office may be covered by privacy of the home (Koops, Schooten & Prinsen, 2004; Buisman & Kierkels, 2014; Koops et al., 2016), because the distinction between personal life and the professional life cannot always be made clearly due to overlap between the two. A relevant factor here could be the type of job, since some professions may complicate the making of this distinction by their very nature (Koops, Schooten & Prinsen, 2004). Presumably, this will only become more difficult with the introduction of more intelligent and smart objects into the home, since more and more processes will be controllable and discernible from both inside and outside the home (Koops & Prinsen, 2015). This may ultimately change the function of the home (Koops & Prinsen, 2015).

One of the problems with privacy of the home is that, while many may have had their reservations or have been alarmed by certain stories about or experienced discrepancies in the usage of intelligent or smart technology, the real awareness of how all their processes increase the 'transparency' of our walls and curtains has yet to find its way to the public at large (Koops, Van Schooten & Prinsen, 2004). This also applies to the information given prior to letting people and technologies into our house: how informed is this consent, really? Has the obtaining of consent been reduced to a mere formality of good form? In the situation that someone would use technology to circumvent the privacy of the home to look into the home or listen in, or access information situated inside the home, this personal freedom would be breached. As pointed out in Part I, technology is becoming more and more sophisticated, and the average individual will not be able to follow the processes and realise when objects inside the home or outside the home are being (mis)used by external actors (Röcker, 2010).

II.1.3 Privacy of person

[9] Article 8 ECHR; Article 7 of the EU Charter is based on Article 8 ECHR, and on the basis of Article 52(3) of the EU Charter, the meaning of this Article within the EU legal framework must not divert from that of the ECHR.

Apart from this elaboration on privacy of the home and the new problems posed to it by the development of the Internet of Things and the 'home invasion' of intelligent and smart objects, other objects of privacy also deserve some attention. The third relevant category for the case assessments is the object 'privacy of person', which covers both the intellect and the body of the individual. Other potential forms linked to this object of privacy are privacy of opinion and expression, privacy of autonomy, and privacy of identity and/or reputation (Koops et al., 2016). Privacy of opinion and of expression serve to some degree as a form of privacy protection, but are often postulated as separate rights, as, for example, in both the ECHR and EU Charter.[10] Nevertheless, these objects of privacy will in the case assessments prove to be very relevant for the protection of privacy. In addition, autonomy has been defined in Part I merely as the ability to make decisions free from (unidentified) externalities, but it is an implied element of privacy as well, as has been pointed out by *inter alia* case law on the general Article on privacy of the ECHR.[11] Since the general Article on privacy of the EU charter is also based on that of the ECHR, the same applies. It is more an inferred right from *inter alia* the general Article, the right to respect for the integrity of body and mind, and freedom of thought, conscience and religion.[12] The close connection between privacy and autonomy is thus apparent from both these European legal instruments. For the purpose of this paper, the focus will be more on the mental side of this category of objects of privacy, in particular privacy of thought, opinion, and decision.

II.2 The case assessments

The objects on which this assessment will be performed are 'Hello Barbie', a lighting system, the smart thermostat 'Toon', and the applications for smart objects for which the focus will be on Fitbit, a fitness tracker which combines wearables, a phone app and an account. For the case analyses, the methodology followed will start with briefly looking into the functionalities of the object of the assessment, and to what extent the object works or has the capability to work autonomously. This will be followed by pointing out some of the impediments of what this means for the autonomy and trust of the individual in respect of usage of the object in question. Finally, the assessment will focus on the aforementioned objects of privacy that are affected by the technological object in question. Here, the aim is to show the overlap of informational privacy with these categories of objects of privacy, while at the same time demonstrate the distinctness of all objects of privacy to illuminate some of the shortcomings of the focus on data protection as the main source of privacy protection in the smart(er) world. Furthermore, the focus will be on the obtaining of information and not on how it is processed after it has been acquired, or the effects of (divergent or wrong) conclusions that may be drawn based upon the information retrieved.

1. 'Hello Barbie'

According to Mattel's fact sheet ("Hello Barbie FAQ", 2015), 'Hello Barbie' is a fashion doll meant as an interactive toy for children from the age of six (manufacturer's recommendation). Children are able to have two-way conversations with this doll, and can play interactive games, since the doll features speech

[10] Articles 9 and 10 ECHR; Articles 10 and 11 EU Charter.
[11] Article 8 ECHR; For example, in *Pretty v United Kingdom*, 2002, as cited by Koops et al. (2016).
[12] Articles 7, 3 and 10 EU Charter.

recognition and is able to 'learn' from 'play history' to tailor conversations, but it does require a WiFi connection to do so ("Hello Barbie FAQ", 2015; Taylor & Michael, 2016; Manta & Olson, 2015). The doll has a button through which it can be turned on; if this is not pressed it should just be a regular Barbie doll, which can be verified simply by checking whether the light of the doll is on ("Hello Barbie FAQ", 2015).

Parents can monitor, and save or delete the 'play history' of the doll with their child via an app that needs to be downloaded first onto a compatible smart object ("Hello Barbie FAQ", 2015). The 'Hello Barbie' doll should be fully controllable by the child and his or her parents, for it cannot turn itself on or collect on its own merits ("Hello Barbie FAQ", 2015). The doll cannot search the Internet or connect with other 'toys', but it can connect to the 'secure' servers of ToyTalk (responsible for the speech recognition technology) in the cloud to access dialogue lines ("Hello Barbie FAQ", 2015; Manta & Olson, 2015). Due to its learning capabilities, it is, however, able to steer the conversation away from past conversations to keep the experience 'fresh' and ask questions ("Hello Barbie FAQ", 2015). Mattel has indicated that these questions will not entail anything inappropriate (e.g. she won't ask for or respond to the child's name and is programmed as to prevent any cussing) nor are they meant to obtain personal information ("Hello Barbie FAQ", 2015). While this sounds reassuring, one reporter who was testing 'Hello Barbie', nevertheless, found that the doll "prompts those conversing with her to divulge information about themselves, but when the focus is on her she quickly changes the subject to invariably gender-normative subjects" (Jason, 2015 as cited in Taylor & Michael, 2016, p. 8).

The doll is thus found to make the child divulge its thoughts and opinions. The child, obviously, has little say in his or her privacy with regard to the usage of the smart toy, nor is it likely that it understands that its privacy is violated by its beloved doll, parents, ToyTalk and everyone ToyTalk provides with access (Taylor & Michael, 2016). This means that not only the privacy of thought and opinion are affected, but also the autonomy and privacy of autonomy. In addition, if the findings of the reporter are true, there could be a problem here with regard to the mental, economic, cultural or social data collected on the child, by which it might be identified.[13] Even if this is not the case, it remains a fearsome violation of privacy and autonomy to monitor everything individuals say in a private environment without their knowledge (Campbell, 2015). The latter is even more problematic when considering that the child lacks the ability to understand this practice, which means that even if the child knew, it would be unable to make the assessment for itself whether the 'cost' of using this smart object is outweighed by the gains. The problem for the privacy of the child here is that informational privacy does not extend to the 'object of protection' under e.g. privacy of thought. The information qualifying as personal data is covered by data protection, but the thoughts, creativity, opinions and beliefs of the child in question uttered in and affected by the 'conversations' with the doll are not. The additional protection of privacy of thought and of autonomy are thus imperative here. Even if it would not be possible to identify the child by the extensive amount of data, it is clear that the other objects of privacy are compromised. The consequences of this practice in the future for the autonomy of the child and its trust in

[13] Article 2(1) Directive 95/46/EC.

his or her environment are not yet known since 'Hello Barbie' has been brought onto the market very recently, though it is hard to imagine that there will be none.

An interesting point of view in this respect is offered by dr. Sherry Turkle, who argued that "sociable robots such as Hello Barbie offer pretend empathy, but they have no empathy to offer because they don't know the arc of a human life. They can deliver only performances of empathy and connection" (as cited in Campbell, 2015). The Hello Barbie doll will thus be partially 'responsible' for the development of a child's understanding of empathising with others, while it is only a commercialised doll. This could clearly interfere with the self-development of the child. The fact that some of the data falls within the scope of data protection does not affect the interference with the self-development of the child in question, nor does it prevent the processing of any data on the child that is not necessarily an identifier. Data protection will thus fall short in protecting the privacy of a child using the Hello Barbie doll.

The same is true for the privacy impediments caused by the gender-normative and superficial lines issued by the 'Hello Barbie' doll. The script of the doll is interfering, steering and influencing the conversations, interests, creativity and overall development of the child (Taylor & Michael, 2016; Gleason as cited in Campbell, 2015), which evidently affects the privacy of autonomy of the child playing with it. This means that the child is pushed to divulge its thoughts and opinions, and then nudged or redirected to the 'right track'. If a child keeps hearing that fashion is important, which seems to be one of the catch phrases of the doll (Taylor & Michael, 2016; Campbell, 2015), it will certainly have an impact on the child's perception of what his or her priorities should be, even if we do not know for sure yet what the repercussions will be. In addition, the doll is being updated regularly to be able to talk about topics that are up-to-date, such as about movies and music artists (Campbell, 2015). This may also affect the decision-making abilities of the child (Koops et al., 2016), since the child does receive information of a commercial nature of *inter alia* movies, music, and topics such as fashion. The doll is provided with the topics to discuss, so the child is naturally directed towards those topics included in the lines ("Hello Barbie FAQ", 2015). The industry would never use this to their commercial advantage, now would they?

While this is already worrisome and problematic, the real danger lies in what is to come. If the main focus would remain on the protection of a limited definition of personal data, what will happen when Hello Barbie evolves, gets 'friends', and a range of smart objects are offered to create the ultimate 'Barbie world'? This may seem dramatic, but not so long ago, the smart Hello Barbie Doll House was introduced. Furthermore, the next logical step is the Hello Barbie dolls being able to talk amongst themselves as well when the child plays with multiple dolls at the same time. The children's room is filling up with devices capable of spying on them, their friends, and on their family. As regard the 'evolving' of Hello Barbie, it might be very possible that it is deemed desirable to make the doll even more 'real', for example, by giving it the ability to respond to certain emotions of children and initiate a conversation on its own merits. Will data protection be up to the task to protect the privacy of the child in question, and everyone close to it?

2. The lighting system

The lighting system that is the object of this case assessment is part of the 'Loxone Smart Home (Loxone, n.d. a). The 'Smart Lighting' of this system is controllable both remotely via an app and manually by

simple switches or a simple remote controller, but it can also function as an autonomous smart system using sensors (Loxone, n.d. a). Different scenes can be selected with Smart Lighting, such as an everyday scene for which lights are triggered when you trigger motion sensors by entering a room (Loxone, n.d. a). These scenes can be adjusted to the preferences of the individual, and can be set for certain parts of the day (or night) (Loxone, n.d. a). Other features are, for example, the ability of the system to initiate the fading of the lights automatically when sensors pick up that the sun is going down, but it remains possible for the individual to change the lighting settings if he or she wishes to (Loxone, n.d. a).

This system was made for a smart home using a central hub, and is thus meant to connect to present smart objects inside the home, which means a great deal of trust is necessary in the technology and the service provided to allow for a partly autonomous system to 'run the home' (Loxone, n.d. b). For example, according to the website, when the individual is not at home but the motion sensors are triggered, it can trigger the alarm and alert the individual to the presence of someone inside the home (Loxone, n.d. a; Loxone, n.d. b). When the sensors are not triggered, the system can turn off other objects in that room (Loxone, n.d. b). Although the system can be controlled without an Internet connection, the ability to access remotely, monitor and control will be limited (Loxone, n.d. b). This means that the individual can control the lighting system with regard to its primary function, which is providing light in the home, but not the connection it makes to other smart objects inside the home or the information it retrieves from these connections and about its own functioning. The central hub is meant to be online at all times supposedly to provide the best service, and to allow for updates to be installed and a current news feed. The information provided on the website indicates that all information is only saved locally on the central hub, but there is no talk about their access to that information (Loxone, n.d. b; Loxone, n.d. c). The "Terms and Conditions" refer only to the "Data Protection Statement" in terms of privacy (Loxone Electronics GmbH, 2013), which in turn only makes reference to personal information such as contact information, and not to collected information inside the home on *inter alia* the usage of 'Smart Lighting' or of the technological objects it is connected to. Moreover, according to the 'Data Protection Statement', the office Loxone Electronics GmbH is responsible for the collection, processing and use of the personal data of their clients (Loxone Electronics GmbH, n.d.).

Even if the promises with regard to the collection, processing and storing of data are true, there is still a lot of data accessible (via the first tier information flow) to the service provider via the central hub about what goes on inside the home when an Internet connection is established. With regard to the lighting system, it relies on sensors that are connected to other smart objects inside the home, as well, which means a lot of information is going back and forth on the behaviour of residents (Loxone, n.d. a; Loxone, n.d. b).

Furthermore, the fact is that the sensors of the lighting system provide a lot of information to external parties and possibly to other residents. The amount of information that can be retrieved from the home without the knowledge of the residents is more extensive than a few decades ago (Koops & Prinsen, 2015). The walls and curtains will not shield residents when the home is becoming 'smarter', and more and more technology is being improved and developed that can be used to enter 'technologically' (Koops & Prinsen, 2015; Koops, Schooten & Prinsen, 2004). Service providers of other smart objects presumably have not made promises about refraining from playing a part in the information flow between sensors, other smart objects, and the central hub. Even if they would, there would be limitations to this 'self-

restraint', since smart objects require a lot of information by their very 'nature'. As pointed out several times already, data protection only has a limited scope, and will thus not cover all data that is processed inside (and possibly via other smart objects outside) the home.

In addition, other residents can look into the central hub and check what everyone else has been up to that day by being able to see, for example, what lighting scenes, rooms and other smart objects have been used. All that information on that central hub inside a home also brings on security risks. The awareness of this potential invasion on the privacy of individuals, more in particular privacy of the home and their behaviour in this private space, may affect the behaviour of residents inside homes with such systems. The realisation that you may be watched, without knowing for sure whether this is the case may add to the overall distrust that could be caused by the increasingly smart(er) environment and the feeling of losing control (Von Locquenghien, 2006 as cited in Röcker, 2010). This sense of distrust may also affect how individuals interact amongst themselves, even inside their own home, rendering the protection of this personal freedom pursued by privacy of the home ineffective in practice (Röcker, 2010; Koops, Schooten & Prinsen, 2004). The protection of personal data will not be able to mitigate the impediments of this practice on privacy of the home and of behaviour, nor on the actual negative effects on the behaviour of individuals inside the home caused by those impediments.

Finally, it must be said that addressing these impediments will only become more pressing as the Internet of Things progresses. One cannot build successfully on a rickety foundation. The more standardised these systems become in homes, and the more smart objects are connected to such systems, the more problematic they will become without sufficient privacy protection. The risk of individuals losing their trust in their surroundings should not be underestimated. Attention for autonomy of the individual and for other objects of privacy than just personal data is of vital importance for their trust in their environment, particularly when it comes to privacy of the home.

3. The smart thermostat

The smart thermostat 'Toon' is a technological object through which an individual can regulate the temperature in the home, and monitor the amount of electricity and gas used (or gained from e.g. solar panels) in the household at all times, in addition to monitoring other devices such as a smart fire alarm or even smart lamps when linked (Eneco B.V., n.d.). It can even help determine which devices inside the home are the least friendly to the overall usage and costs of your energy consumption (Eneco B.V., n.d.). The smart thermostat requires a WiFi connection, and needs to be linked to the gas or electricity meter reader and central-heating boiler. It can be fully operated directly through the screen of the device itself, but if considered desirable, it can also be controlled remotely through other smart objects in the house such as via a tablet or iPhone for which an app can be downloaded (Eneco B.V., n.d.).

This particular smart thermostat is mostly part of a service contract, for which the privacy statement says that the necessary personal information can be collected, processed and stored (Eneco N.V., 2016a), but nothing is said about their direct access to information situated on the thermostat. For the app to control the smart thermostat remotely, the only additional article on privacy entails that the usage of the app requires the company to send the personal information established by the thermostat to the smart devices on which you have installed the app (Eneco Consumenten B.V., 2015). It does not turn itself on or off, since it is meant to be on at all times, but it collects all the data on your energy

consumption autonomously. If the thermostat is linked to other smart objects, it may in addition collect data with regard to the usage of those objects, but this is not shared with the company itself unless the individual has given his consent hereto (Eneco B.V., n.d.; Eneco N.V., 2016a). Nevertheless, other smart objects need to be linked to the thermostat by the individual him or herself, and so far, it should only be possible for a determined number of objects in line with the services provided by the thermostat, namely the smart fire alarm, hue smart lamps, solar panels, and smart plugs ('Koppel Toon® aan slimme apparaten', n.d.; Eneco Customer Service, personal communication, August 19, 2016). This is a positive development in respect of the autonomy of the individual versus the autonomy of the thermostat, since the individual has control over which other smart objects inside and around the home the thermostat can connect to.

In addition, all the collected data can be accessed and deleted by the human operator from the smart thermostat, yet data remains accessible for the service provider (Eneco Consumenten B.V., 2015; Eneco N.V., 2016a; Eneco Customer Service, personal communication, August 19, 2016). However, due to the lack of adjustable privacy settings and the vague, broad terms in the subsequent privacy statements on the possibility that something may or may not be accessed or transmitted to the provider, it is not possible for the individual to discern whether this has occurred. In addition, the fact that it is not possible to personalise privacy settings on a device as such, with such a potentially prominent role in the home, nor follow the (content of the) information flow, does not really add to the privacy and trust of the individual in his or her environment (Eneco Customer Service, personal communication, August 19, 2016).

It could be argued that any type of moderately autonomous object that is intelligent or smart would affect autonomy and trust. Whether these objects would be encroached upon would then depend on whether its functioning corresponds to the actual wants and needs of the individual (Mik, 2016), instead of to those towards which the individual was pushed by unidentified externalities (Brownsword, 2011; Baldwin, 2014 as cited in Mik, 2016). In this case, the thermostat is a smart object, but it does not think for the individual; it is meant to support the individual by providing him or her with more insight into his or her consumption and costs to enable the individual to make a more informed decision and thereby increase control. When this thermostat is compared to the 'Nest', the latter thermostat is a lot smarter in the sense that it can learn what the habits and preferences are of the individual, while 'Toon' cannot (Hijink, 2016). With a smarter thermostat such as 'Nest', it can only accommodate the needs and preferences of the individual if the individual lives a very predictable, routine life (Hijink, 2016). The autonomy of the individual is preserved more by 'Toon' since he or she can program the preferences and alter them when the individual desires to do so.

Furthermore, a smarter thermostat such as 'Nest' could become even more problematic for the autonomy and trust of individuals in their environment if there are several residents in one home (Denning, Kohno & Levy, 2013): whose needs and wants should be accommodated? In the latter case, this could have significant ramifications for the trust the individual has in its environment, since he or she has trouble controlling what happens inside his or her own home, especially when more smart objects are connected to such a system capable of directing the household to such an extent (Röcker, 2010). The latter consideration is the main reason why trust is vital for smart objects and central systems such as the central hub discussed above and the smart thermostat Nest. If it works properly and is able to foresee the

individual in all his or her needs, desires (within reason) and increase control, and its functioning can be followed and understood by the individual to a certain degree, it will mitigate some of the trust issues and reserves individuals may have about smart(er) environments.

Due to these similarities between the lighting systems discussed above and this smart thermostat, the same privacy considerations are relevant with regard to privacy of the home and behaviour of individuals. Therefore, it is more beneficial to focus on other (potential) impediments for privacy, autonomy and trust in this case assessment. With regard to behaviour inside the home, the smart thermostat 'Toon' provides users with the opportunity to compare their energy consumption to that of other 'Toon' users in their neighbourhood. Although there do not seem to be any publicly known cases or complaints in this regard, it seems only likely that individuals will start to compare and alter their behaviour when the energy consumption by neighbours is much less or much higher, even if it is not possible for individuals to determine the identity of those neighbours. Notwithstanding the fact that a race to the bottom could be a positive consequence, it does seem quite similar to nudging, which is a popular subject in ethics. Even if it would be 'good', which is a matter of perspective, forcing or influencing people in such a way as to make them make different choices without them realising the degree to which externalities have guided them towards those decisions affects both the autonomy and behaviour of the individual inside his or her own home (Brownsword, 2011; Baldwin 2014 as cited in Mik, 2016). Although this example may not seem that intrusive, the object of this analysis is not just situated in the home, but is also capable of partially running it. As argued above, such an object requires a great deal of trust in order for it to effectively accommodate the individual. If you were to consider the fact that our trust is put in a smart object that is of such potential prominence in arguably the ultimate private space, while it is capable of directing our decisions, opinions and behaviour inside that space without most of us being able to identify its 'push', one may start to feel a bit more uneasy about the power such a smart object has. This is all the more true when more smart objects make it into the home capable of being linked to the smart thermostat. Apart from the lack of privacy settings, Toon is now still very much under the control of individuals. This may change when its range and compatibility with other smart objects increases inside the house, just as with the lighting system.

The fact that all this information is accessible to the service provider via the smart thermostat, and that some of this information (though anonymised) is shared with other Toon-users compromises not only the information about other objects of privacy identified as relevant here, but also the area beyond that. It is not just about the information; the objects of privacy such as the decision-making and behaviour of the individual inside the home is not protected by data protection unless it entails personal data (Koops et al., 2016). Admittedly, most of the time individuals provide external actors with the access to their personal information themselves, but that does not mean that they have given up on their privacy and consent to have those service providers make extensive and invasive profiles on them. An individual may not mind sharing bits and pieces, but while single act alone may not say much about an individual, the compilation of everything that goes on inside a home certainly can. There is a reasonable expectation of privacy inside the home, even if the services of third parties are used. Presumably, the overall emerging practice to entrust third parties with personal information is key to the present-day mobility of both the individual and their information. Admittedly, trusting third parties such as Google as a safe keeper of personal information may indeed affect the reasonable expectation of privacy negatively (Koops, 2011; Mik,

2016), but the mere use of the services of a third party in this way in itself should not. This mobility of individuals and information is essential to the success of the smart world, and is also one of the key objectives of the European Union. However, there is still a lot to be said about the variating trustworthiness of third parties (Mik, 2016; Koops, 2011). As aforementioned, these new technologies and services are not just a new or updated version of what once was; they are technological developments capable of bringing on significant changes in society in both behaviour and communication (Koops, 2011). This may simply be one of them. This should not affect the reasonable expectation of privacy an individual has in the home when such services are used, especially not when one considers the power gained by some parts of the private industry over the years.

4. Fitbit

Fitbit is a fitness tracker that can be used to monitor the number of steps the human user has taken, and provide guidance on weight and nutrition goals (Hilts, Parsons & Knockel, 2016; "Why Fitbit", n.d.). In addition, it can provide the human user with insight into personal health information such as the individual's heart rate or the quality of sleep, although this does not include gender specific features such as the menstrual cycle (Hilt, Parsons & Knockel, 2016). Fitbit is meant to empower individuals to maintain a 'fit' lifestyle or improve it (Hilts, Parsons & Knockel, 2016; "Find Your Fit", n.d.).

The nature and extensiveness of the information collected depends on the type of wearable Fitbit device(s) used ("Fitbit Privacy Policy", 2014; Hilts, Parsons & Knockel, 2016). The wearables are able to track the footsteps of the individual with their sensors, and "when combined with those integrated with mobile phones …, which are often accessible by installed fitness tracking mobile applications, can often be used to automatically collect far more information [than] just footsteps" (Hilts, Parsons & Knockel, 2016, p. 6). The wearable Fitbit device uses Bluetooth to transmit the data it has collected to the Fitbit app, which can be installed on devices such as the smart phone or computer ("Fitbit Privacy Policy", 2014). The Fitbit devices have a screen, as is also required of the device on which the app can be installed or the account is managed ("Let's Get Down", n.d.). While Fitbit does not allow for privacy settings, the individual using Fitbit should know exactly what he or she shares: everything ("Fitbit Privacy Policy", 2014; Weinstein, 2015; Maddox, 2015). Alongside all that the wearable is able to register of what the individual does, this fitness tracker also collects personal data such as the age, weight and gender of its user (Macdonald, 2016; Hilts, Parsons & Knockel, 2015). The Fitbit device automatically synchronises stats wirelessly via a Bluetooth connection to *inter alia* the phone on which the app is installed or via the individual's account, as well as to the Fitbit servers ("Fitbit Privacy Policy", 2014).

Furthermore, according to the privacy policy of Fitbit location features need to be activated to be available, but the devices have fixed identifiers and are not endowed with Bluetooth Privacy ("Fitbit Privacy Policy", 2014; Macdonald, 2016; Hilts, Parsons & Knockel, 2016; Weinstein 2015). When the Bluetooth connection is turned off the devices can still be traced via the fixed identifiers of the wearables, and leak information (Macdonald, 2016; Hilts, Parsons & Knockel, 2016, 2015; Weinstein). There have also been cases of informational leakage, for example, in 2011 profiles of Fitbit users were publicly visible via a Google search due to the fact that the owners of those profiles did not recognise what the default privacy settings of Fitbit entailed (Weinstein, 2015; Rao, 2011). In addition, when the wearables transmit information all log data is collected ("Fitbit Privacy Policy", 2014), and when custom workout

mapping features are being used, or have just been used, location information is transmitted over the Internet as well (Hilts, Parsons & Knockel, 2015). Despite the fact that it is possible to delete some types of information on the individual's Fitbit, with some services it requires the deletion of those services entirely ("Fitbit Privacy Policy, 2014), while for others it is found to be a complex process due to the interconnectedness of databases (Maddox, 2015). Even when the wearables are not worn, Fitbit is able to register the inactivity of the wearable, and if the individual has not undertaken any action to unable these processes, can still track the individual to some degree through other sensors such as of a smart phone with the app. The individual thus can protect his or her own privacy somewhat by taking additional action, but is generally unable to exercise 'control' over his or her Fitbit in its functioning and data collecting if the individual wants to continue to use its services (Maddox, 2015). Furthermore, it is of note to mention the conclusion drawn by Adamic (2015) that Fitbit compromises the individual's own analysis and awareness of his or her own body since the fitness tracker provides the individual with information on his or her physical needs based on quite basic and limited information. This is a very interesting find when considering the individual's autonomy and the trust required by Fitbit of the individual in its processes. Fitbit can tell the individual to exercise more while he or she may already be in optimum condition, or that he or she has had a bad night of sleep before he or she may even realise it by him or herself. Due to the quantity of information provided (and collected) by Fitbit on the body of the human user, this could result in the individual just 'taking Fitbit's word for it'. The individual could start acting accordingly, while he or she may not have acted differently had the individual not been told that he or she was tired. Another example would be that the human user of Fitbit is basically told over and over by using Fitbit what he or she does wrong, which will undoubtedly affect the thoughts, opinions and ultimately the behaviour and decisions made by the individual. However, the extent to which may vary largely from individual to individual. Also, this is not necessarily negative, since one of the motives to use Fitbit seems to be the desire to be more aware and to get pushed more in order to achieve a healthier lifestyle (Malhorta, 2015; Adamic, 2015), but the fact remains that the awareness and autonomy of the individual is compromised.

Hilts, Parsons and Knockel (2015) explain that one of the reasons to conduct their research was the trust issues expressed among consumers in relation to the extensive data collection (not the autonomous functionalities), and with the considerations above in mind, it seems that there are indeed plenty of reasons to justify consumer's concerns in this regard. In addition, Fitbit "retains personally identifiable information (PII) as long as a user maintains an account, and only deletes accounts after individuals contact the company's support agents requesting a deletion" (Hilts, Parsons & Knockel, 2015, p. 43). While their definition if personal data is broader than just contact information, which is in fact positive for the individual's data protection, it falls within their discretion to determine whether something is capable of pointing towards a particular individual in respect of the extensive amount of data that is shared by the human actor using Fitbit. As has been found by some, Fitbit does not consider most of the data shared by the individual as 'personal', which is apparent from their privacy terms on the amount of 'wiggle room' they have allowed themselves in handling the collected information (Weinstein, 2015; "Fitbit Privacy Policy", 2014). Moreover, the large amount of data collected may be pseudonymised, or even anonymised, but when profiles contain a lot of detailed information, it seems likely that many of these profiles could be connected to certain human users. This is likely to increase in

the near future, since both our phones and the wearables of Fitbit become more sophisticated and smart with each updated version, so the data collected may increase as well in both its quality and quantity.

Arguably, if the same *ratio* as in the other case assessments is applied, this also affects the privacy of thought, autonomy and behaviour, and privacy of the home. Individuals are encouraged to insert goals and additional personal information about themselves, including what is important to them and what they want to achieve ("Fitbit App", n.d.; "Fitbit Privacy Policy", 2014). However, the thoughts and opinions themselves, again, are not protected under data protection. On the contrary, they may not be linkable to a specific human user, which means that Fitbit's privacy terms would not identify it as personal identifiable information, and neither does European data protection law, both under the regime of the Council of Europe and in the EU. However, the fact that the chances are slim that a person can be identified by information consisting of thoughts and opinions does not mean that the individual wants that type of products of the mind to go further than him or herself, without being able to control what happens to it after it is inserted. Privacy of thought definitely goes further than just the information about its object.

Moving on, the next relevant object of privacy is privacy of the home, because this fitness tracker does not stop when the individual enters his or her home. It is more than likely that a wearable that (with a little help from possibly the human user's phone) tracks every move of the user will also catch him or her doing a lot of intimate activities, like bathroom breaks and activities of a procreative nature, but also general information such as on what floor you are. The more connected sensors and the better the quality of them, the more specific information can be collected on the way the individual moves, and what combinations of movement, altitudes, breathing, and even standstills mean. This is interesting, since the EU "outlaws, in the absence of proper legal safeguards, the processing of 'sensitive' data, such as on a person's … health, or … sexual life." (European Union Agency for Fundamental Rights, 2014, p. 16).[14] Furthermore, it may also affect the behaviour of individuals inside their own home for the same reason. The individual may alter his or her behaviour (unconsciously) due to the 'awareness' of being monitored all the time. This may be the desired effect by some, but it is also important to consider that an alternative motive would be the fact that the individual desires to keep certain things hidden.

Another possible object of privacy that might be of relevance here is the body: while it is not the movement of the individual him or herself or touching of the body by others that is restricted, it is the information on the functioning of the body, and what activities are conducted to explain the functioning of the body. All this information together certainly makes for a higher probability of an individual being identified. Even if this would not be possible legally, this information could technically be matched to medical records in certain cases. In that case, European data protection law would apply,[15] but the protection does not extend to the privacy of the body. Apart from identifiability, the mere fact that such information can generally be found in medical records already testifies of the personal nature of information on bodily functioning. Even in the cases that the information could not lead to an individual being identified, it is obvious that individuals using Fitbit have a genuine "interest in the privacy of their

[14] Article 6 Convention 108.

[15] See Article 2(a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

physical body" (Koops et al., 2016). It is thus important that the bodily privacy beyond the limited definition of personal data is not overlooked in order to be able to protect these privacy interests of the individual.

Obviously, even when the individual gives Fitbit quite a blank consent with regard to the information on him or her, Fitbit may not do whatever it wants with the information that is collected, but it is clear that their practices are not contributing to the protection of privacy of the individual. It is interesting to see that so many objects of privacy are relevant for the usage (and actions of) Fitbit, but worrying that there are so many aspects that have the potential to be harmful for the autonomy and trust of the individual, and above all to the privacy of the individual, both with regard to data as beyond. Whether Fitbit's services actually infringe the privacy of individuals using them depends largely on the case, in which relevant factors would be *inter alia* the nature and extensiveness of the information shared and the manner in which Fitbit has handled this information. It seems almost tedious at this point to point out data protection is clearly unable to protect the other objects of privacy affected by Fitbit. Due to the extensive amount of information that is collected, it really depends on how detailed the profiles are, and how they are structured.

5. Analysis of the case assessments

Arguably, there are important differences and similarities between some of the examples relevant for the concept of privacy beyond the screen inside the home. This showed the relevance of the factors taken into account in the general analysis for the variations both in autonomy of the individual and technological object, and the ramifications for the privacy of the individual and his or her trust in his surroundings. The focus of attention is centred too much on the development of technology and surveillance in public, instead of on the development of 'strengthening' the walls of our homes that are becoming more transparent with every intelligent or smart object that is brought into our homes.

In addition, by analysing for each technological object which objects of privacy were relevant, the significance of sufficient and separate protection of the objects of privacy, and the inability of data protection law to protect the individual for privacy beyond privacy of information was demonstrated (Koops, 2011; Cuijpers, Leenes, Olislaegers & Stuurman, 2011). Arguably, for some categories more than others, the concerns expressed with regard to privacy inside the home in our smarter world have been found justified. Smart objects do not necessarily affect the autonomy of the individual, but both the general analysis and the case assessments showed that it is likely that it does. The question should be: to what extent is the compromised autonomy and privacy of the individual acceptable? The answer to this question is vital to shape privacy beyond the screen and autonomy in the smart home. Since this question is not a simple one, more research is therefore required to prepare the present for tomorrow.

CONCLUSION

The smarter technological objects become, the more autonomous their functioning will be. When the functioning of an intelligent or smart object corresponds to the actual wants and needs of the human user (within reasonable limits), the mere fact that the human user does not need to tell the object to do so should not constitute a problem for the autonomy of the individual (Mik, 2016). Unfortunately, a lot of impediments have been found that suggest that the individual is often directed into a direction by

externalities (Brownsword, 2011; Mik, 2016; Harris, 2016; Akrich, 1992 as cited in Howcroft, Mitev & Wilson, 2004). Furthermore, even if an object is capable of serving the individual efficiently and properly, there is a price to pay by the individual for all the intelligent and smart technology, both in time spent and by providing external actors with access to information about the individual (Harris, 2016; Mik, 2016). This is especially problematic due to the home invasion of smart and intelligent objects, while the concept of privacy beyond the screen inside our home has not received much attention (see Helal, et al, 2015; Kortuem, Kawsar, Sundramoorthy & Fitton, 2010).

In this paper, it was argued that the concept of privacy beyond the screen inside the home needs to be broken down in categories in order to determine some of the relevant factors necessary to demonstrate both the importance and problems of this concept. The obvious question to tackle is: what constitutes a screen? To make the distinction between smart or intelligent technological objects with a screen and those without, it depends *inter alia* on the extent to which an object without a screen is operated and controlled via another device with screen for the former object to still qualify as being without a screen. When the object cannot be operated without the 'control device' with screen, it then comes down to whether the control device allows for privacy settings to be individualised for the dependent object. With regard to smart or intelligent objects with a screen, a further analysis is necessary on the degree of sophistication of the screen. If the screen is too basic, in the sense that it does not allow for the individual to adjust privacy settings, it can still qualify as a technological object relevant for the concept of privacy beyond the screen. It is thus not merely the presence or absence of a screen on the object or control device that is relevant, but the possibility for the individual to exercise some control over the information in and/or output of a device, regardless of whether this is provided for directly via the screen of the technological object itself, or indirectly via the screen of another smart or intelligent object. In addition, monitoring capabilities of those objects relevant for the concept of privacy beyond the screen inside the home could be of note, as well. When the individual cannot personalise the privacy settings or other related functionalities, the possibility for him or her to at least see the extent of information that is collected and determine the information flow of the smart object inside and outside the home to a certain degree gives the individual more insight into the 'cost' of using the technological object, and thereby allows for the individual to make a more informed decision. However, due to all the (for the individual generally unidentifiable) externalities influencing the decision making of the individual, regardless of whether they are built in the technology or pressures from e.g. a societal nature, the ability for the individual to make decisions autonomous has become more questionable (Mik, 2016). To determine the extent of autonomy with which the technological object functions, the monitoring capabilities can also be looked into from the perspective of the industry. In combination with the foregoing, this is relevant to establish whether the technological object is gaining autonomy at the expense of the autonomy of the individual, and whether the industry itself is still able to 'control' the functioning of the object or the information flow. These considerations are especially of significance for the privacy and autonomy of the individual inside his or her own home, due to the importance of the home for privacy (Koops et al., 2016) and the increasing inability for the individual to protect him or herself in the increasingly smarter environment. Moreover, there are additional ramifications for the trust an individual has in his or her surroundings the more the individual's autonomy is affected negatively, as well as for privacy when processes become both harder to control and understand. This paper has attempted to demonstrate the

latter statement by first zooming in on the home, as arguably the ultimate example of space covered by privacy, to show that the rapid technological developments have gained quite the head start when compared to privacy protection.

Privacy protection has not been at a complete standstill, since the protection of personal data has received significant attention, and rightly so considering that the information flow has reached new proportions, both quantitatively and qualitatively. Nevertheless, it seems obvious that the current focus on informational privacy does not prepare us for the excessive and omnipresent data capturing and processing that is (a necessary) part of the smart(er) world (Röcker, 2010; Koops, 2011; Koops, Schooten & Prinsen, 2004). The problem is that the other objects of privacy protection seem to have suffered of being underestimated in their relevance or being put on a backburner. The new technological developments of the past decades and those already standing at the gates are not just updates or replacements of older versions, their social and economic impacts are greater and new (Koops, 2011; Röcker, 2010). "[It] is important to be aware, that the designs, that dominate early in the growth of a technology, can have disproportionate power over the way the technology will affect social life" (Rheingold, 2003 as cited in Röcker, 2010, p. 65). With these considerations in mind, the conclusion to draw is that the protection of personal data, while imperative, cannot replace the protection of other objects of privacy. Data protection alone cannot address these developments in protecting the individual efficiently and properly in the near future. The case assessments further underlined both the differences between the objects of privacy and their interconnectedness, and above all, their significance today and tomorrow. The question to ask now is: to what extent is the compromised autonomy and privacy of the individual acceptable? With our whole lives available on the Internet, our increasing inability to act and decide autonomously and understand what goes on in our surrounding due to our increasingly smarter environment, it seems that it is time for us to become smarter, too, and re-evaluate the protection of privacy and autonomy inside the home.

BIBLIOGRAPHY

Adamic, J. [Johnny Adamic]. (2015, May 4). The Dark Side of Your Fitbit and Fitness App [Blog Post]. Retrieved from http://www.thedailybeast.com/articles/2015/04/05/the-dark-side-of-your-fitbit-and-fitness-app.html.

Bohn, J., Coroamă, V., Langheinrich, M., Mattern, F., & Rohs, M. (2004). Living in a Word of Smart Everyday Objects – Social, Economic, and Ethical Implications. *Human and Ecological Risk Assessment 10*, pp. 763-785. Retrieved from http://www.vs.inf.ethz.ch/publ/papers/hera.pdf.

Brownsword, R. (2011). Autonomy, Delegation, and Responsibility: Agents in Autonomic Computing Environments. In Hildebrandt, M., & Rouvroy, A. (Ed.), *Law, Human Agency and Automatic Computing* (pp. 64-84).

Buisman, S.S., & Kierkels, S.B.G. (2014). Commentaar op Artikel 12 van de Grondwet. In Hirsh Balin, E.M.H., & Leenknegt, G. (Ed.), *Artikelsgewijs commentaar op de Grondwet* (Web edition 2016). Retrieved from http://www.nederlandrechtsstaat.nl/grondwet/artikel.html?artikel=12##artikel12.

Campbell, M. (2015, December 1). Hell No Barbie: 8 Reasons to Leave Hello Barbie on the Shelf. Retrieved from http://www.commercialfreechildhood.org/action/hell-no-barbie-8-reasons-leave-hello-barbie-shelf.

Cohen, J.E. (2008). Privacy, Visibility, Transparency, and Exposure. *University Chicago Law Review 75*, pp. 181-201. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1012068.

Cook, T. (2016, February 16). A Message to Our Customers. Retrieved from http://www.apple.com/customer-letter/.

Cuijpers, M.K.C., Leenes, R., Olislaegers, S., & Stuurman, K. (2011). *De Wolk in het Onderwijs. Privacy Aspecten bij Cloud Computing Services* [White Paper]. Retrieved from the Cooperation SURF E.A. website: https://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2011/De_wolk_in_het_onderwijs_feb2011.pdf.

Davy, A. (2003). *Components of a smart device and smart device interactions* [White Paper]. Retrieved from the M-Zones website: http://www.m-zones.org/deliverables/d234_1/papers/davy-components-of-a-smart-device.pdf.

Denning, T., Kohno, T., & Levy, H.M. (2013). Computer Security and the Modern Home. *Communications of the ACM 56:1*, pp. 94-103. doi:10.1145/2398356.2398377.

Dobbins, D.L. (2015). *Analysis of Security Concerns & Privacy Risks of Children's Smart Toys*. Retrieved from https://sever.wustl.edu/degreeprograms/cyber-security-management/SiteAssets/Dobbins%20-%20SmartToy_Security_Final%20Revised%209-28-15.pdf.

Eneco (n.d. a). *Koppel Toon® aan Slimme Apparaten*. Retrieved from https://www.eneco.nl/toon-thermostaat/slim-huis-met-toon/.

Eneco (n.d. b). *Voor de Allesweters.* Retrieved from https://www.eneco.nl/toon-thermostaat/meer-weten/

Eneco Consumenten B.V. (2015). *Voorwaarden voor de Toon® App van Eneco*. Retrieved from http://www.eneco.nl/-/media/eneco/pdf/actie/voorwaardentoonoptablet.ashx?la=nl-nl.

Eneco N.V. (2016a). *Privacyverklaring Toon® van Eneco.* Retrieved from http://www.eneco.nl/-/media/eneco/pdf/voorwaarden-en-brochures/voorwaarden-overig/enecotoonprivacyverklaring.ashx?la=nl-nl.

Eneco N.V. (2016b). *Aanvullende Privacyverklaring Toon®.* Retrieved from http://www.eneco.nl/-/media/eneco/pdf/toon-thermostaat-support/aanvullendeprivacyverklaringtoon.ashx?la=nl-nl.

Eskens, S., Timmer, J., Kool, L., & Est, R. van (2016). *Beyond control. Exploratory study on the discourse in Silicon Valley about consumer privacy in the Internet of Things*. Rathenau Instituut, Den Haag. Netherlands.

European Commission (2009). *Guidance Document No. 11 – On the Application of the Directive on the Safety of Toys (88/378/EEC)*. Retrieved from https://law.resource.org/pub/eu/toys/guidance/011-guidance-children-3-years-en.pdf.

European Commission (2016). *Reform of EU data protection*. Retrieved from http://ec.europa.eu/justice/data-protection/reform/index_en.htm.

European Data Protection Supervisor (2015). *Opinion 4/2015 - Towards a New Digital Ethics*. Retrieved from https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-09-11_Data_Ethics_EN.pdf.

European Parliament (2015). *Big Data and Smart Devices and Their Impact on Privacy*. Retrieved from http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL_STU(2015)536455_EN.pdf.

European Union Agency for Fundamental Rights (2014). *Handbook on European Data Protection Law*. Retrieved from http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf.

Find Your Fit. Retrieved from http://www.fitbit.com/nl/whyfitbit.

First Chamber of the Dutch Parliament (1998). *Verklaring dat er grond bestaat een voorstel in overweging te nemen tot verandering in de Grondwet van de bepalingen over het binnentreden in woningen*. Kamerstukken I 1997/98, 25 442, nr. 231b. Retrieved from https://zoek.officielebekendmakingen.nl/dossier/25442/kst-19971998-25442-231b?resultIndex=5&sorttype=1&sortorder=4.

Fitbit Privacy Policy. (2014). Retrieved from https://www.fitbit.com/nl/privacy.

Harris, T. (2016). How Technology Hijacks People's Minds: From a Magician and Google's Design Ethicist [Blog post]. Retrieved from https://medium.com/@tristanharris/how-technology-hijacks-peoples-minds-from-a-magician-and-google-s-design-ethicist-56d62ef5edf3#.fzgnn6whl.

Helal, S., Mann, W., El-Zabadani, H., King, J., Kaddoura, Y., & Jansen, E. (2015). The Gator Tech Smart House: A Programmable Pervasive Space. *Computer 38:3*, pp. 50-60. DOI: http://dx.doi.org/10.1109/MC.2005.107.

Hello Barbie FAQ (2015). Retrieved from http://hellobarbiefaq.mattel.com/faq/.

Hijink, M. [Marc Hijink] (2016, 26 April). Vakkundig verrast door Toon [Blog post]. Retrieved from https://www.nrc.nl/nieuws/2016/04/26/vakkundig-verrast-door-toon-1612458-a880165.

Hilts, A., Parsons, C., & Knockel, J. (2016). *Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security* (Open Effect Report 2016). Retrieved from https://openeffect.ca/reports/Every_Step_You_Fake.pdf.

Howcroft, D., Mitev, N., & Wilson, M. (2004). What We May Learn from the Social Shaping of Technology Approach. In Mingers, J. and Willcocks, L. (Ed.), *Social Theory and Philosophy for Information Systems* (pp. 329-371). Retrieved from http://eu.wiley.com/WileyCDA/WileyTitle/productCd-EHEP000971.html.

Hsiung, H., Scheurich, S., & Ferrante, F. (2001). Bridging E-Business and Added Trust: Keys to E-Business Growth. *IT Professional 3:2*, pp. 41-45. Retrieved from http://home.himolde.no/~molka/lo205/booknotes-06/bank-encryption-00918219.pdf.

Hung, P.C.K., Fantinato, M., & Rafferty, L. (2016, June). A Study of Privacy Requirements for Smart Toys. Paper presented at the *Pacific Asia Conference on Information Systems*. Retrieved from http://www.pacis-net.org/index.php?year=2016.

Jones, M.L., & Meurer, K. (2016). Can (and Should) Hello Barbie Keep a Secret? *IEEE Ethics 2016*. Retrieved from http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2768507.

Khamooshi, A. (2016). Breaking Down Apple's iPhone Fight With the U.S. Government. *New York Times*. Retrieved from http://www.nytimes.com/interactive/2016/03/03/technology/apple-iphone-fbi-fight-explained.html?_r=0.

Kharpal, A. (2016, March 29). Apple vs FBI: All You Need to Know. *CNBC London*. Retrieved from http://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html.

Kilkelly, U. (2001). *The Right to Respect for Private and Family Life*. Germany. Retrieved from https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168007ff47.

Kim, D.J., Song, Y.I., Braynov, S.B., & Rao, H.R. (2005). A Multidimensional Trust Formation Model in B-to-C e-Commerce: A Conceptual Framework and Content Analyses of Academia/Practitioner Perspectives. *Decision Support Systems 40*, pp. 143-165. Retrieved from http://wings.buffalo.edu/academic/department/som/isinterface/papers/A%20multidimensional%20trust%20formation.pdf.

Koops, E.J. (2011). Digitale Grondrechten en de Staatscommissie: Op Zoek naar de Kern. *Tijdschrift voor Constitutioneel Recht*, pp. 168-185. Retrieved from http://www.tvcr.nl/tijdschriftvoorconstitutioneelrecht/download/69Digitale_grondrechten_en_de_Staatscommissie.pdf.

Koops, E.J., & Prinsen, M.M. (2015). Glazen Woning, Transparant Lichaam. Een Toekomstblik op Huisrecht en Lichamelijke Integriteit. *Nederlands Juristenblad*, pp. 624-630. Retrieved from https://www.recht.nl/doc/lichaamenhuis.pdf.

Koops, E.J., Newell, B.C., Timan, T., Škorvánek, I., Chokrevski, T., & Galič, M. (2016). A Typology of Privacy. *University of Pennsylvania Journal of International Law, Vol. 38 (2016)*. Retrieved from http://ssrn.com/abstract=2754043.

Koops, E.J., Van Schooten, H., & Prinsen, M.M. (2004). *Recht naar Binnen Kijken: Een Toekomstverkenning van Huisrecht, Lichamelijke Integriteit en Nieuwe Opsporingstechnieken*. Den Haag, Netherlands: SDU Uitgevers.

Kortuem, G., Kawsar, F., Sundramoorthy, V., & Fitton, D. (2010). Smart Objects as Building Blocks for the Internet of Things. *IEEE Internet Computing 14:1*, pp. 44-51. DOI: http://dx.doi.org/10.1109/MIC.2009.143.

Lahlou, S., Langheinrich, M., & Röcker, C (2005). Privacy and Trust Issues with Invisible Computers. *Communications of the ACM 48:3*, pp. 59-60. DOI: http://dx.doi.org/10.1145/1047671.1047705.

Let's Get Down to Specifics. Retrieved from https://www.fitbit.com/nl/devices.

Loxone (n.d. a). Smart Lighting. Retrieved from http://www.loxone.com/enen/smart-home/everything-managed/lighting.html.

Loxone (n.d. b). See How Loxone Works. Retrieved from http://www.loxone.com/enen/smart-home/how-it-works.html.

Loxone (n.d. c). The Heart of Home Automation. Retrieved from http://www.loxone.com/enen/products/miniserver/miniserver.html.

Loxone Electronics GmbH (2013). Terms and Conditions. Retrieved from http://www.loxone.com/enen/t-and-c.html.

Loxone Electronics GmbH (n.d.). Data Protection Statement. Retrieved from http://www.loxone.com/enen/purchase/data-protection-statement.html.

Selling Wearables Are 'Leaking' Data Even When Turned Off. *The Daily Mail UK*. Retrieved from http://www.dailymail.co.uk/sciencetech/article-3429067/Is-fitness-tracker-putting-privacy-risk-Claims-selling-wearables-leaking-data-turned-off.html.

Maddox, T. (2015). The Dark Side of Wearables: How They're Secretly Jeopardizing Your Security and Privacy. *Tech Republic*. Retrieved from http://www.techrepublic.com/article/the-dark-side-of-wearables-how-theyre-secretly-jeopardizing-your-security-and-privacy/.

Malhotra, A. [Aseem Malhotra]. (2016, May 15). Take off that Fitbit. Exercise alone won't make you lose weight [Blog Post]. *The Washington Post*. Retrieved from https://www.washingtonpost.com/posteverything/wp/2015/05/15/take-off-that-fitbit-exercise-alone-wont-make-you-lose-weight/?utm_term=.04e510d02147.

Manta, I.D., & Olson, D.S. (2015). Hello Barbie: First They Will Monitor You, then They Will Discriminate Against You. Perfectly. *Alabama Law Review 67:1*, pp. 136-187. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2578815.

Meijers, A. (2011). Overheidsverantwoordelijkheid in het Informatietijdperk: Een Pleidooi voor het Creëren van Genormeerde Experimenteerruimte. In Broeders, A., Cuijpers, M.K.C., & Prins, J.E.J. (Ed.), *De Staat van Informatie* (pp. 97-132). Retrieved from http://www.oapen.org/search?identifier=375125.

Mevis, P.A.M. (2014). De Bescherming van de Woning 25 Jaar Later. In Hofstee, E.J. et al. (Ed.), *Kringgedachten. Opstellen van de Kring Corstens* (pp. 157-170). Retrieved from http://repub.eur.nl/pub/77214/.

Mik, E. (2016). The Erosion of Autonomy in Online Consumer Transactions. *Law, Innovation and Technology 8:1*, pp. 1-38.

Milaj, J. (2015). Privacy, Surveillance, and the Proportionality Principle: The Need for a Method of Assessing Privacy Implications of Technologies Used for Surveillance. *International Review of Law, Computers & Technology*. Retrieved from DOI: 10.1080/13600869.2015.1076993.

Pierson, D. (2016). FBI vs. Apple: How Both Sides were Winners and Losers. *Los Angeles Times*. Retrieved from http://www.latimes.com/business/technology/la-fi-tn-apple-fbi-explainer-20160329-snap-htmlstory.html.

Poslad, S. (2009). *Ubiquitous Computing: Smart Devices, Environments and Interactions*. Chichester, United Kingdom: John Wiley & Sons Ltd.

Rao, L. (2011, July 3). Sexual Activity Tracked by Fitbit Shows Up In Google Search Results. *Tech Crunch*. Retrieved from https://techcrunch.com/2011/07/03/sexual-activity-tracked-by-fitbit-shows-up-in-google-search-results/.

Röcker, C. (2010). Social and Technological Concerns Associated with the Usage of Ubiquitous Computing Technologies. *Issues in Information Systems 11:1*, pp. 61-68. Retrieved from http://iacis.org/iis/2010/61-68_LV2010_1428.pdf.

Shin, D. (2014). A socio-technical framework for Internet-of-Things design: A human-centered design for the Internet of Things. *Telematics and Informatics 31* (2014) 519–531. Retrieved from http://www.sciencedirect.com/science/article/pii/S0736585314000185.

Streitz, N. et al (2005). Designing Smart Artifacts for Smart Environments. *Computer 38:3*, pp. 41–49. DOI: http://dx.doi.org/10.1109/MC.2005.92.

Taylor, E., & Michael, K. (2016). Smart Toys that are the Stuff of Nightmares. *IEEE Technology and Society Magazine*, pp. 8-10. DOI: http://dx.doi.org/10.1109/MTS.2016.2527078.

Weinstein, M. (2015, December 21). What Your Fitbit Doesn't Want You to Know. *The Huffington Post*. Retrieved from http://www.huffingtonpost.com/mark-weinstein/what-your-fitbit-doesnt-w_b_8851664.html.

Wynsberghe, Aimee Van (2012). *Designing Robots with Care: creating an ethical framework for the future design and implementation of care robots*. (Unpublished PhD dissertation). University of Twente, Twente, Netherlands.