Trust in the networked era

Keymolen, Esther

Published in:
Techné: Research in Philosophy and Technology

DOI:
10.5840/techne201792271

Publication date:
2018

Published in: Techné: Research in Philosophy and Technology
22:1 (2018): 1–25

DOI: 10.5840/techne201792271

Trust in the networked era: When phones become hotel keys

Esther Keymolen[1]

Abstract: This article is an update of Latour's well-known case of the unreturned hotel key. In recent years, the hotel key has been replaced by a keycard and more recently by a digital key that can be downloaded on a smartphone. This article analyses how—with every step in the innovation process—the trust relation of hotel owner and hotel guest is mediated in a distinct way. The networked ontology of the digital key enables the collection of personal information from which the hotel can tailor its services to the wishes of the hotel guests. While this may be in the interest of the guest, it, however, also makes the guest vulnerable as she has only limited control over the data and comes to depend on the conduct of the hotel. The digital key is not merely a key to open a hotel door; it also unlocks the personal information of the guest.

Key words: trust, Latour, hotel keys, privacy, technological mediation

1. Introduction

The history of modern hotels allegedly started in 1862 with the opening of the marvellous Le Grand Hotel in Paris (Ambrosino 2014).[1] With 800 rooms and beautiful architecture, the Grand Hotel set a new standard in the hotel sector. The Grand Hotel's key policy was a prime example of the way in which modern hotel businesses should be run. Metal keys were "attached to a big key-ring, which was hung on a board at the concierge office" (Ambrosino 2014, 3). Consequently, guests had to visit the concierge first in order to obtain their key and to turn it in, as guests were not allowed to take keys outside of the hotel.

[1] Esther Keymolen, eLaw Center for Law and Digital Technologies, Leiden University, Steenschuur 25, 2311 ES Leiden, The Netherlands; e.l.o.keymolen@law.leidenuniv.nl

It may not come as a surprise then to know that hotel guests quite often forgot to hand their key in at the front desk. Obviously, they were more concerned with visiting the "City of Lights" rather than returning their keys. As a result of this understandable, but still irresponsible behaviour, hotel owners were faced with *issues of trust*. Were they fooling themselves if they kept on relying on the guests to return their hotel keys?

The problem of unreturned hotel keys has been elaborated by sociologist and philosopher Bruno Latour (Latour 1990, Latour 1992, 104) who shows how a weight attached to the room key may persuade the hotel guest to return it to the hotel desk, making it easer for the hotel owner to trust the hotel guest with the key.[2] With this example, Latour aimed to show that artefacts should be taken into account when it comes to analysing interactions as it is specifically the connection between actants—human and nonhuman alike—that accounts for what takes place in interaction. It is not just the responsibility of the hotel guest to return the key. The responsibility can be distributed between the hotel guest, the key, and the added weight. Hence, to analyse trust one has to take into account the agency of the artefact mediating the interaction.

While it is true that the weight attached to the hotel key has had a significant impact on hotel practices, innovations in the hotel sector did not end here. In recent years, there has been a shift from *keys* to *keycards*. The introduction of keycards enables a different kind of interaction from that of the "old-fashioned" hotel keys as Latour described them. Because a new keycard can easily be printed, it diminishes the problem of forgotten keys. This article will show how the keycard pre-sorts a specific kind of trust relation between the hotel owner and the hotel guest, differing from the previous relation mediated by the traditional, metal hotel key.

The main focus of this article, however, will be on the newest, state-of-the-art hotel key, which actually is no longer a key or a card, but a smartphone. In 2014, the high-end hotel chain Hilton invested 500 million dollars in the development of a digital environment culminating in an app, which not only makes it possible for a customer to select a specific room in the hotel and pre-order extra services, but which also turns a telephone into a digital key (Hilton 2014). By waving a smartphone in front of the lock, the door opens. This innovation, however, also opens up the possibility for excessive data gathering and data analysis, again changing the interaction of hotel owners and their guests in new ways.

This article will show how the trust relation of hotel owner and hotel guest evolves with every new step in the innovation process of the hotel key. In order to detect these changes, the focus lies on specific artefacts with a specific design functioning within a specific social context. This approach is central to the *empirical turn in the philosophy of technology* (Achterhuis 2001). As this article focuses on the role of trust in the relation of hotel guest and hotel owner, it can be classified as a *society-orientated* analysis in the philosophy of technology. Nevertheless, it also strongly adheres to the basic starting point of the *engineering-orientated* approach in the philosophy of technology, which states that in order to analyse the mediating effects of artefacts, we need to have a clear understanding of the technology at hand (on the distinction between society-orientated and engineering-orientated philosophy of technology see Brey 2010, 39-40).

This article, therefore, explicitly takes a practical, contextual approach to interpreting the different stages of the hotel key (also see Kaplan 2009, 1). When it comes to networked artefacts such as the digital key, this contextual approach entails an analysis not only of the way in which the hotel guests *perceive* the digital key, but also includes an analysis of what takes place *behind the interface*. While hotel guests may base their trust in the digital key on the fact that the app is easy to use and has a slick design, the network of actants behind the interface, out of sight for the hotel guests, may have interests that do not align with those of the hotel guests. Moreover, the extra technical functionalities of the digital key, which may enable excessive data gathering, monitoring, and profiling of hotel guests, may render the hotel guests more vulnerable than was the case with the predecessors of the digital key.

It has to be noted that the trust relation of hotel owner and hotel guest does not merely revolve around a hotel key. The relation is in fact much more complex and both the hotel owner and the guest may have to deal with other trust issues as well. For instance, the hotel owner has to trust the guest to behave properly within the hotel and not to bother other guests. In turn, the guests have to trust the hotel owner not to enter the room without their permission and to have taken sufficient security and safety measures to ensure a safe stay in the hotel.

This article will focus only on the trust relation mediated by the key and the network of actants the key brings together. In its most elementary and basic form, a trust relation consists of three elements: A trusts B to do X (also see Hardin 2006, Kohn 2008). In the case of the key, this brings us to the following trust relation: the hotel owner (A) trusts the hotel guest (B) to return the key (X). However, as we will come to see, the agency of the key is not limited to merely opening and closing doors. With every step in its development, it pre-sorts the trust relation of hotel owner and hotel guest in a significantly new way. And as a result, the initial trust relation changes as well.

2 The hotel key and a cumbersome but handy key chain

In different writings, Latour makes a convincing plea to not forget the nonhumans when analysing social interactions and to truly overcome the modern dichotomy of object and subject (Latour 1992, Latour 1993). This dichotomy Latour localises—amongst others—in strong social constructivism (Brey 2009, 102, also see: van den Berg 2009, 32) as well as in phenomenological accounts (Latour 1993, also see Verbeek 2000, 180-188) despite of their claimed intentions to overcome the divide.

Latour develops a theory, or better, a set of concepts that could replace the "technology/society" divide by instead focusing on *generalised symmetry*. The basic idea is that humans and nonhumans can only be understood through the networks that connect them. An artefact only gets meaning through the interaction with humans, and humans become who they are by their interaction with artefacts. Following Latour (1990, 103), to understand the way power relations work in society, we, therefore, also have to take into account the nonhuman actants and the way in which they persuade and mobilise other actants to display certain behaviour in social links. To illustrate how nonhumans are part of power relations and how all networked actants influence each other, Latour comes up with the example of the hotel owner who seeks a way to persuade their guests to bring back the hotel keys (Latour 1990, Akrich and Latour 1992).

2.1 The problem of missing keys

Latour (1990, 103) describes how the hotel owner kindly requesting guests to leave their key at the front desk did not seem to have much effect on the guests. Also, a sign with the explicit inscription "please leave your room key at the front desk before you go out" did not result in the behaviour demanded by the hotel owner. It is only when an "innovator" comes to the rescue and "displaces the inscription by introducing a large metal weight, the hotel manager no longer has to rely on his customer's sense of moral obligation" (Latour 1990, 103).

What happens here cannot easily be understood by upholding a rigorous distinction between humans and nonhumans. To understand how a bulky keychain changes the behaviour or "program of action" of both human (i.e. hotel owner, guests) and nonhuman (i.e. the key, the weight) actants, one has to see how "the original program of action is thus translated or transformed in the technical mediation into a new one" (Verbeek 2000, 173).

The program of action of the hotel manager is "I want the hotel guests to bring back their keys" which may be in conflict with the program of action of the guests which are more focused on "having a nice holiday." The latter is an anti-program because it does not align with the intentions of the hotel owner. The hotel owner can now try to connect with other actants to fortify their message. They can add an oral message to their wish: "Please Miss. Anderson, can you return the key when you leave the hotel?"; the hotel owner can put up a sign with the same message; and they can attach a cumbersome weight to the key.

Every time, the hotel owner includes a new actant in the chain of mediation, they try to persuade the hotel guests to adapt their program of action. In order for them to be successful and establish a predictable, stable interaction with their guests, not necessarily all but most anti-programs have to be countered. Returning the keys then becomes something, which people just do, without really thinking about it or questioning the request.

The initial message "return the keys when you leave the hotel" is no longer the same because of the associations taken by the hotel manager. It has been *translated.* By displacing the message using the weight they have added to the key, the message has become transformed. The key together with the weight attached to it substitutes the hotel manager's demand for returning the keys. The design of the key weight helps the hotel guest return the key to the front desk. It is no longer something the hotel guests have to do by themselves; it is partly *delegated* to the bulky key chain. In these associations of humans and nonhumans, changes occur. Because of their connectedness, they are no longer the same entities. As Latour describes: "The statement is no longer the same, the customers are no longer the same, the key is no longer the same—even the hotel is no longer quite exactly the same" (Latour 1990, 105).

2.2 Conceptualising trust

In order to analyse this initial step in the innovation process of the hotel key from a trust perspective, we have to wrap our mind around the concept of trust itself first. Trust is generally perceived as an important strategy to deal with the uncertainty inherent in human life (Luhmann 1979, also see: Möllering 2006) and plays an important role when it comes to accepting new technologies (McKnight, Choudhury, and Kacmar 2002, McKnight and Chervany 2002, Kiran and Verbeek 2010). Simultaneously, the way in which trust is being established is also shaped by the artefacts involved (Kiran and Verbeek 2010). Defining trust in a strict sense is, however, very difficult if one does not want to lose the richness of the phenomenon (Simon 2013).

In line with Ludwig Wittgenstein (2009 [1953], 67), I have, therefore, chosen to look for "family resemblances," instead of trying to come up with a conclusive definition of what trust is. I have focused on a *family of related concepts* that I found chiefly in the work of Niklas Luhmann (Luhmann 1979, 1988) who is generally perceived as one of the key authors in trust research (Seligman 1997, 18, Möllering 2006, 5, Taddeo 2009, 24) and more recently in the work of Guido Möllering (2001, 2005, 2006).[3] In their interrelatedness, they form the conceptual lens that will be put to use to analyse the evolving trust relation of the hotel owner and hotel guest. The family of related trust concepts consists of: *reducing complexity, positive expectations, trustor, trustee, agency, vulnerability, social context.*

2.2.1 A family of trust concepts

Trust, as Luhmann sees it, is a way to *reduce complexity* that is inherent in the social world human beings inhabit (for an extensive analysis of the need for trust to cooperate in a social world see: Simpson 2012). This complexity enters the human world by means of two elements: the other and time, revealing a social and a temporal level in the complexity of the world.

Human beings are aware of the world's contingency. Without some sense of trust, they would be overwhelmed by the idea of all the possible turns fate could take. In the present, they have to cope with an over-complex future. Therefore, trust has to do with anticipating the future. Trust is "to behave as though the future were certain" (Luhmann 1979, 10).

Because of this future-orientatedness, trust is closely tied to *expectations*. Possible fulfilment only appears after the action has taken place, while commitment has to be there beforehand. To trust is to have *positive expectations* concerning the future actions of other actors.

Social complexity enters the scene because of the fact that we, as human beings, cannot exactly predict the thoughts and actions of others, they are—to a certain extent—black boxes to us and, consequently, constitute a source of insecurity. When an actor *(the trustor*) trusts another actor (*the trustee*), they generally have positive expectations of the intentions or behaviour of this person. The relevance of trust is due to the principal *vulnerability and uncertainty* of the trustor towards the trustee. There is always something at stake. Luhmann (1979, 42), therefore, refers to trust as a "risky investment." Because the trustor does not know for sure how the trustee will act, the trustee can *harm* the trustor (idem, 8).

However, it is not merely that the trustor does not have all the information about the intentions of the trustee, but also that both are actors with a certain amount of autonomy; they have *agency*. This also means that trust *cannot be forced or guaranteed*. Finally, another important aspect is to recognise that the trustor and the trustee are embedded in a *social context* which influences how exactly they can define themselves as actors and enact their agency (Möllering 2006). Luhmann speaks of a "familiar world." Trust can only take place in a familiar world in which existence is already structured in a pre-reflexive way. Our experience of the world automatically entails the intersubjective constitution of meaning.

2.3 Trust between the hotel owner and the hotel guest

Making use of this family of related trust concepts, it now becomes possible to retell Latour's analysis of the forgotten keys focussing on the issue of trust. The hotel owner (*trustor*) has to deal with the complexity of not knowing for sure if the guests (*trustees*) will return the key to the front desk as they are supposed to. In the transaction of giving the key to the guest, there is *something at stake*. If the hotel owner wants to have a flourishing hotel business, they are bound to providing the guest with a key, running the risk of losing the key if the guest does not return it. Of course, there are some checks and balances in place (*social context*). The guest has handed over their personal information to the hotel owner, making it possible to identify and trace them if something might go wrong. Moreover, the guest has signed a contract, agreeing to act according to the rules set in the hotel policy. Still, the hotel guest has the freedom to act (*agency*) in a way that is in conflict with the *expectations* of the hotel owner, making the hotel owner *vulnerable* nonetheless. Trust can never be forced or guaranteed. In that sense, trust is always blind trust. It entails the suspension of looking for more evidence, more certainty, and accepting the uncertainty inherent in every social interaction (Möllering 2006). Trust is a fiction necessary to face reality. The hotel owner providing the hotel guest with the key acts *as if* they are sure about the way in which the guest will behave, while in fact they are not.

Unfortunately for the hotel owner, this trust is often shattered, because of the absent-mindedness of careless hotel guests. In an effort to turn the tide, the hotel manager calls in the help from an innovator who comes up with the plan to add a weight to the key in order to make it physically less attractive for guests to take the key with them when leaving the hotel. Also, in this new relation of the hotel owner and the innovator trust issues arise. The hotel owner has to trust the innovator to come up with a successful plan to persuade the guests. Next, when this innovation is adopted in the interaction of hotel owner and guests, it also becomes an object of trust—of system trust, more precisely (for an analysis of 'system trust' see: Luhmann 1988, 1979, Giddens 1991, Giddens 1990, Giddens and Pierson 1998). The hotel manager then not only has to trust the guests, but also has to have confidence in the way in which the keychain functions.

Finally, after adding the heavy keychain to the key, most of the guests adapt their behaviour and bring back the key. Although the interaction has changed because of the introduction of the weight attached to the key, it remains an interaction where trust is present. Trust is now *distributed trust*, as the trust first uniquely vested in the hotel guest is now shared between the hotel guest and the key with weight; or even more specifically, it is invested in the new *association* of hotel guest + key + weight.

Although guests display more trustworthy behaviour because of the bulky keychain, they can still breach the trust of the hotel owner and take the key with them when they leave the hotel. In the altered relation, guests still have agency, which is a precondition for trust. If it could be possible to completely control the returning of the keys, trust would be redundant. Thus, although their actions are more predictable now that they interact with the bulky keychain, hotel guests can still act differently than expected and hoped for by the hotel owner.

3. When a key becomes a card

In the example of Latour, the cumbersome keychain is a material strategy to persuade hotel guests to display trustworthy behaviour. Another strategy, however, could be not to try to change the behaviour of the hotel guests, but to see if it might be possible to rearrange the situation in such a way that there is *less at stake* for the hotel owner. In other words, if it is possible to provide the guest with a key which when not returned does not impose too much of a burden on the hotel owner, consequently *resolving the complexity* involved. As we have seen, trust is always a risky business. If there is less to be risked, then there is less need for trust as well. By making use of the *family of trust concepts*, we can analyse how the hotel key card shapes the trust relation of hotel owner and guest.

The hotel key card is a plastic card, generally having the looks and size of a credit card that can be programmed to open a specific door for a certain period of time. If it is returned to the front desk, it can—depending on the type of card—often be reused by overriding the initial data and putting new data on it. If the hotel guest (*trustee*) does not return the key card, the costs to replace it by a new card are substantially low. As a result, in this new situation there is less at stake for the hotel owner (*trustor*). With the introduction of the key card, the hotel owner becomes less *vulnerable* to breaches of trust. The hotel owner no longer needs to have *positive expectations* of the guest's behaviour. By replacing the traditional key with a reusable card, it simply no longer matters whether or not the guest returns the key.

Moreover, an additional benefit of the hotel card is that the physical privacy of the guests is assured more than in the situation with the "normal" key.[4] If, in the past, a key was not returned, the only way to fully ensure the privacy of the room was to change the lock and buy a new key. This obviously is a time consuming and costly solution. More times than not, the key would merely be replaced by a copy. Consequently, the hotel guest who still possessed the key could access the room long after they were allowed to do so, or even worse sell the key on the streets. Indeed, in the 1960s and 1970s, these keys were sold on the black market for $500 (Sherry 1993, 355). Due to the fact that in general the name of the hotel and the number of the room was printed on the key chain, it was quite easy to make illegal use of such stolen keys.

In the case of the key card, however, when a card is lost or not returned, a new card can easily be printed. The physical privacy of the room will be less compromised as it is only in the time between losing the card and replacing it that unauthorised individuals can open the door, and furthermore, if and only if they would be able to trace the matching room number, which is generally not printed on the card. Moreover, as there is no identifying information visible on the card, and since it does not contain identifying information, the informational privacy also seems well taken care of. The positive expectations of the hotel guest, i.e. the hotel owner provides them with a safe place to stay, will most likely be realised. As we have seen, trust always implies vulnerability and uncertainty; there has to be something at stake. By replacing the metal key with a plastic key card, vulnerability has been substantially reduced not only for the hotel owner who no longer needs to rely on the guest to bring back the key, but for the guest whose physical as well as informational privacy is better protected as well.

Is trust no longer existent in the interaction between hotel owner and guest, then?

Trust has not become redundant. The interaction of hotel owner and hotel guest is certainly not completely defined by the transaction of the key or key card. The hotel owner also still expects the guest not to cause any annoyances for other guests and to respect their property. Alternatively, the guest still expects the hotel owner and staff to honour their privacy by not entering the room without the guest's permission. Moreover, the key card also brings along *new complexities* that both hotel owner and hotel guest have to cope with. The hotel owner has to trust their suppliers to provide them with reliable cards and a reliable system; the hotel guest has to become familiar with the way the cards work (how to put them in the card reader and to make sure they do not get damaged).

All in all, the introduction of the key card did alter the trust relation, but not because it led to a new distribution of trust—as was the case with the adding of the key chain weight—but because it reduced the vulnerability of the hotel owner and helped to establish a familiar, predictable world (*social context*).

4. When a key card becomes a smartphone

On 28 July 2014, the prominent hotel company Hilton announced that as part of extending their customized digital services to hotel guests, they would make it possible for guests to use their phones as a key to open the lock of their hotel door.

These new services would, amongst others, enable customers to choose a specific room (i.e. a room in which they had stayed before), pre-order services, skip the check-in at the front desk, and let them go straight to their room. Similarly, other hotel chains, such as Starwood Hotels & Resorts (SPG) and Hyatt Hotels and Resorts, started testing the possibility of using a smartphone to open doors (White 2014).

We started this article with a mundane metal hotel key that went missing more often than the hotel owner was willing to accept. Now, we find ourselves engaged with *the hotel key of the networked era*: no longer a key, but a phone. Increasingly, the Internet becomes integrated in a wide range of artefacts we use in everyday life. These artefacts become *embedded in networks of information* often *invisible* to the user. Mere physical objects become what has been framed as *smart* by adding a computational component to them, bridging the gap between the physical world and the online world (Kopetz 2011, 308). By integrating the functionality of a key—opening doors—into the workings of a smartphone, the keyless key is a prime example of the *connectedness, personalisation*, and *pro-activity,* which has been declared central to today's networked era (Floridi 2012, The-Online-Initiative 2015, Mayer-Schönberger and Cukier 2013).

In the networked era, smartphones are becoming mundane artefacts themselves. Recent reports (Ericsson 2016) foresee that by 2021 there will be 6.3 billion smartphone users accounting for more than 70% of all mobile traffic. It is to be expected that more and more companies will provide all sorts of personalized and pro-active services via smartphones and that because of the increasing use of smartphones, even more people will gain access to these services. Hence, where the keyless key is now still part of the privileged domain of the high-end hotel chains, this innovation will most likely trickle down and impact the hotel sector as a whole, just as the case with previous hotel key innovations. Moreover, as the keyless key is part of an overall shift towards providing personalized and pro-active services via smart artefacts, some of the challenges brought forth by the digital key as discussed in the next part of this article can also be found in other apps and services.

In order to grasp the mediating workings of the digital key and its impact on trust, we start the analysis with the experience of the hotel guest (4.1). What aspects are being *amplified* by the interface and what is *hidden* from sight for the hotel guests (Ihde 1990, Verbeek 2011)? The way in which the interface of the app is designed, its ease-of-use, and the options the guests have to adapt the app all influence their trust in the digital key.

Taking into account Latour's generalized symmetry, the next step is to analyse the digital hotel key as an actant, which—because of its networked character—brings along several new actors and interests. In 4.2 and 4.3, we, therefore, look into the functioning and security of the app, the managing system, and the connected interests of the hotel owner. This approach is loosely based on a conceptual framework developed in Esther Keymolen (2016).

4.1 The experience of hotel guests

How do hotel guests interact with the hotel and its staff when the digital key becomes an integral part of their stay at the hotel?

First, guests have to download the designated application (app). Next, when the app has been installed and a reservation has been made, the guest can opt to request a digital key. The guest will receive a push notification with the room number and the digital key—which comes in the form of encrypted code—on the day of arrival. The guest can then go straight to the room, avoiding the check-in at the hotel's front desk. By waving the phone close to the lock on the door, the door can be opened.

In addition to the digital key, the app also allows guests to personalise their stay. They can choose—making use of digital floor plans—which particular room they want and they can pre-order all kinds of services. Moreover, the hotel can send them push notifications with all sorts of special offers. Generally, these apps are designed in a way that they can be used and navigated intuitively. Hotel guests don't need a manual to understand the way in which they can make use of the digital key.

Previously, a test was conducted in the Clarion Hotel in Stockholm to collect feedback of guests on the use of digital keys (see Pesonen and Horster 2012, 14-15). The results showed that: participants appreciated not having to check in and out, that they all saved on time, almost all participants indicated that they would use digital keys, and the majority of the guests also declared that "the service made their hotel stay more pleasant" (Brown 2011). Before starting their new digital services, the Hilton chain initiated a survey in order to become aware of the wishes of their clients. They found that 84% were in favour of choosing their own room and two out of three wanted more control over the room where they stayed (Odedra 2015). In addition, Barbara Neuhofer, Dimitrios Buhalis, and Adele Ladkin (2015, 249) found that the possibility to personalize the stay of the hotel guest through the digital key app was an important innovation.

Notwithstanding all these positive expectations concerning the digital key and the supporting smartphone application, some uncertainties from a user's perspective also arose concerning the use of these digital hotel services. Brandon Ambrosino (2014), for example, wonders what the impact of the keyless key may be on the guest's interaction with hotel staff. Where Neuhofer, Buhalis, and Ladkin (2015) chiefly focus on the personalised experience made possible by smart technology, Ambrosino (2014) questions if digital keys will just lead to more impersonal hotel experiences. Moreover, where the digital key may add to the experience of specific hotel guests—such as business people or tech-savvy guests, it might actually be a burden for people who share a room such as travelling families. Finally, also on the level of security problems may arise. Whereas in the situation of the old-fashioned metal key, problems arrived because of the negligence of the guests, now problems may arise because guests create easy-to-break passwords, not being fully aware of the consequences it has when their phone suddenly becomes more than just their phone, but a way to gain access to their personal domain. The guest's phone becomes more valuable and, therefore, also more attractive to steal or hack.

4.2 The digital key as a system

While the guests interact with the interface of the app, all the technical processing is conveniently tucked away behind the sleek and intuitive design of the interface. Moreover, the smartphone is inherently connected via the Internet to other actants such as the *locks* and the *managing system* of the hotel. This network of actants remains out of sight of the direct experience of hotel guests. Hotels as well as the system suppliers do their uttermost best to protect the technical specifics of their proprietary technologies (Manley 2015).

As a result, the hotel guests are not directly confronted with the technical workings of the app or with the values that are embedded in the app, nor can they easily assess the security of these technical processes. These technologies, therefore, often remain black boxes for hotel guests as well as for researchers. Nevertheless, as a point of reference, this article focuses on the lock systems of supplier ASSA ABLOY, as it not only is one of the global leaders in lock systems, but is also the supplier of the

Starwood Hotels and Resorts chain, one of the first hotel companies to introduce the digital key.

4.2.1 NFC and BLE

The locks of ASSA ABLOY that connect with the smartphone work with RFID (Radio Frequency Identification) as they first had to interact with RFID key cards. These locks, often installed above or next to the door handle, make use of radio frequency electromagnetic fields to read and identify objects with a tag, such as a RFID key card. Currently these locks are being upgraded to become compatible with NFC (Near Field Communication) and BLE (Bluetooth Low Energy) technology.

NFC is a “short range and wireless technology for data transfer without physical touch” (Pesonen and Horster 2012, 11) and it is increasingly being integrated into electronic devices such as the iPhone 6, iPad mini 3, and the Apple Watch. This latter gadget even has its own integrated hotel app, which apparently is compatible with the lock system of the Starwood hotel chain (Boden 2015).

BLE is a low-power technology developed for short-range control and monitoring applications (Gomez, Oller, and Paradells 2012, 11734). BLE can be built onto the existing Bluetooth infrastructure, making it easy to adopt (Gupta 2013, 7-8). One of the most promising BLE-enabled applications is the so-called beacon. These often-small devices send out a unique identifier to a compatible app or device in the vicinity, after which a certain action can be triggered or a push notification can be sent. Apple, for instance, uses iBeacons in its stores to provide users: extra product information tailored to the products the customers are looking at in a specific part of the store, special offers, and the opportunity to pay for the products through their phone, skipping the line in front of the checkout. In a similar fashion, beacons can also be used on hotel premises.

Both BLE and NFC are deemed to be secure, with NFC being the most secure because of its proximity requirements. More than NFC, BLE runs the risk of interfering with other transmissions and it is also more vulnerable to DDOS (Distributed Denial Of Service) attacks.

For the hotel business, the longer range of BLE is nevertheless very attractive as BLE beacons integrated in the hotel environment enable them to collect data about the whereabouts of their guests. These data can be used to enhance and personalise the stay of the hotel guest or —as we will see in 4.3—be monetised by selling the data to third parties.

4.2.2 Managing systems

Functionality is also of the utmost importance when looking at property management systems (PMS) of hotels. Increasingly, all necessary hotel operations—from checking in guests, maintenance, security etc.—are brought together in one property management system. Also, ASSA ABLOY offers a modular system, giving hotels the possibility to build a system tailored to their needs and wishes. Therefore, while it might be true that this data mostly stays within the property management system (Mitchell 2006), the smartphone converts itself functioning as a source of new data by transmitting data on the activities of the guest in the hotel to the management system.

In general, hotel owners do claim that “the locks and mobile keys are designed to as be equally secure as traditional room keys” and that they “prioritise guest and property safety above all else” (Manley 2015). However, they do not provide concrete information, leading to superlative, but rather trivial messages on the security of their products (see for example: ASSA-ABLOY 2015, 6). Harry Sverdlove (cited in White 2014), chief technology officer of the cyber security firm Bit9, comments that when it comes to security in the hospitality industry, the biggest challenge is that convenience trumps security. In order to ensure a positive guest experience, a system has to cater to a variety of needs making it necessarily very flexible and, therefore, also more vulnerable to breaches. All in all, it seems that when it comes to security, hotel guests simply have to trust the hotels and their system suppliers to have invested in appropriate technical security measures.

4.3 The interest of the hotel owner

To understand hotel companies’ reasons for developing and implementing digital keys, one has to take into account the more encompassing trends in the hospitality sector. These trends are, not surprisingly, linked to dominant, technological developments in society of offering more personalised and pro-active services via digital tools. Personalisation can be perceived as

> a form of user-to-system interactivity that uses a set of technological features to adapt the content, delivery, and arrangement of a communication to individual users' explicitly registered and / or implicitly determined preferences. (Thurman and Schifferes 2012, 776)

The basic idea behind personalisation in the business domain is that it will lead to better customer relations and consequently more revenue for the companies involved. Or, as Hilton Worldwide's global head of digital services Geraldine Calpin (cited in: Odedra 2015) puts it:

> Everything we do is designed to better serve our guests so they are more loyal to our brands –including digital tools - thereby driving business and generating revenue for owners. We expect a high return on investment from the digital tools driven by increased brand loyalty and incremental revenue from push notifications, upsell opportunities and pre-arrival requests.

A necessary condition to pro-actively cater to the personal needs of customers via these digital tools is the collection and analysis of large quantities of—personal—data. The gathering of data has already been part of hotel processes for quite some time. Through customer relationship management services (CRS), hotels collect information about guests. This information is not limited to what happens within the hotel—whether or not guests make use of room service, the restaurant, special offers, if there are incidents, …—but may also include information retrieved online (Lindberg 2013). Taking into account the privacy policy of the Hilton hotel, the conclusion can be short: "at every touch point or guest interaction" personal information may be gathered.[5] This information includes—amongst others—contact information, personal characteristics, nationality, income, passport number and details, such as place of issue, travel history, etc. It may also include the collection and keeping of information and records "related to conversations, including recording or monitoring customer service calls."[6]

Personal information may also be obtained from third parties such as from airline and credit card partners, as well as information derived from social media sites. It may also be shared with affiliates, franchisees or business partners of the hotel. And the information will be retained as long as needed to fulfil the goals for which it was collected, unless the hotel is obliged by law to retain it for a longer period of time.

With the arrival of the hotel app and—as a new part of that–the digital key, also *geo-location* information can now be added to the CRS database. Moreover, by also making use of beacons, guests–who have downloaded the designated app–can be tracked and followed when they move around in the hotel. This information can not only be used to monitor hotel operations–for example, if there is a queue in the restaurant–but beacons can also be programmed to send push notifications with special, targeted offers to the guest's smart phone, when they are, for example, nearby the pool or cafe.

Again, the rationale behind this targeted advertising is that customers who are approached in a personalised manner and are presented offers tailored to their needs will be more likely to accept the offer than they would when receiving merely generic offers. However, as Frederik Borgesius (2014, 36) notes in his research on online behavioural targeting, there is no consensus on the effectiveness of targeted advertisement (compare Chen and Stallaert 2014).

It has to be noted that hotel guests have to agree with the terms and conditions of the app and that the privacy policy is of course available to read through. However, research convincingly indicates that people seldom actually read these documents (Schermer, Custers, and van der Hof 2014). Even if they take the time to read them, it is doubtful whether they would be able to fully understand their content because of the legalese language in which these documents are generally drafted.

The introduction of the digital key is, rather than the baseline, the icing on the cake when it comes to the collecting of data. It can be seen as a new strategy in the longer tradition of hotels to gather information on their customers. With the arrival of the digital key, not only is a new tool being added to the hotel's arsenal of monitoring instruments, but also a new sort of information is being collected: geo-location data. Moreover, the digital character of the collected information enables the hotel to not only collect, but also combine, analyse, and share the data, bringing forth questions concerning privacy and accountability.

From a user's perspective, digital tools are designed to give guests the desired "choice and control" over their stay (Odedra 2015). From the hotel owner's perspective, digital tools help to create personalised and pro-active services, which in the end must lead to more revenue for the hotels.

4.4 Revised and repeated: Trust between the hotel owner and the hotel guest

Whereas in the introduction of the bulky keychain, trust became distributed between the guest + key + chain, the use of the key card decreased the vulnerability of the hotel owner, making trust less needed as a way to deal with the uncertain behaviour of hotel guests. With the arrival of the digital key, trust becomes important once again, as the complexity within the interaction rises, through the arrival of a monitoring system that facilitates the collection of data and the pro-active services based on these data. Through the lens of the family of trust concepts, it is now possible to assess how trust between hotel guest and hotel owner takes shape in the relation mediated by the digital key.

The experience of the hotel guest

From a user's perspective, we see that hotel guests are provided with an application that enables them to tailor their stay to their own preferences. The interfaces of the hotel apps are generally designed in such a way that they are easy to use and self-explanatory (Morosan and DeFranco 2015, 123-124). Ostensibly, this leaves hotel guests with more control and, therefore, less *complexity* to resolve. By circumventing the hotel owner at the front desk, it seems as if the interaction between hotel owner and hotel guest-and the *vulnerability* attached to this interaction–no longer takes place; seemingly all is dissolved into a digital piece of transferable code. It now merely revolves around a hotel guest opening the door of their temporary private domain with their phone. The hotel owner has, so to speak, left the building, and the digital key has apparently replaced their interpersonal interaction. As a result, trust shifts from the interpersonal level to the artefact, to the system itself. As the direct interaction between hotel owner and hotel guest has vanished, trust is no longer to be found at the front desk of the hotel, but in the interaction of the hotel guest with the digital key.

Can the digital key be trusted? As Joseph Pitt (2010) rightly points out, this question is too broad to be answered in a meaningful way. We can only come up with such an answer by referring to *specific actions* of the digital key. However, the hotel guests only have a limited perception of its actions. Because of its user-friendly interface and slick design, they are not directly confronted with all the technical workings of the digital key app. They are generally not aware of the presence of the actants behind the interface–such as the hotel owner and the supplier–nor can they assess to what extent the interests of these hidden actants are in line or in conflict with their own interests. This lack of awareness makes their assessment of the digital key one-dimensional, resulting in contemplations such as: Can the digital key be trusted to open the door? Can the digital key app be trusted to always be accessible? In terms of the family of trust concepts, the guests' *positive expectations* are only related to the recognizable functionality of the digital key, and do not take into account the functionality that is hidden behind the interface.

However, when we look at the construction of the digital key, it becomes clear that its functionality is not limited to the opening and closing of the hotel door and that it actually is because of these extra functionalities that the hotel guests become *more vulnerable* than was the case before.

Where in the past, it was first and foremost the *hotel owner* who had to bear the uncertainty of not knowing if customers would return the hotel key, now the *vulnerability* increasingly lies with the *hotel guest*. Where the hotel through the collection of information comes to know its guests a lot better (making the future more predictable and therefore less complex), what exactly happens to and with this data lies beyond the knowledge and influence of the hotel guest.

Moreover, new actants are added to this relation now. The manufacturer and its monitoring system that is connected to the digital key increasingly pre-sort the action space of the hotel guest. It is the system connected to the digital key that sets the boundaries for the interaction, and to a certain extent prescribes what the hotel guest may and may not do. As these are often proprietary systems, manufacturers are not transparent about their functioning, nor are they willing to share much information on the level of security. This, again, makes the hotel guest more vulnerable.

New trust relations mediated by the digital key

We started this article with the basic trust relation revolving around an old-fashioned metal key: the hotel owner trusts the hotel guest to return the key. However, with the arrival of the digital key other trust relations occur. When we look at the experience of the hotel guest, the main trust issues are related to the functioning of the key. Can the hotel guest trust the digital key to properly open and close the hotel room door? Beyond any doubt this is an important question as it relates to the hotel guests' physical privacy and safety, which largely depend on the proper functioning of the digital key. However, this is not the only thing that is at stake.

As our analysis shows, hotel guests become more vulnerable due to the excessive gathering of personal information and the arrival of new actants with interests that not necessarily align with those of the hotel guests. This new vulnerability relates to the informational privacy and safety of the hotel guests and potentially turns around the trust roles of hotel guest and hotel owner. Because vulnerability is being shifted towards the hotel guests, they take the role of *trustor*, while the hotel owner and other connected actants become the *trustee*. The hotel guests have to trust the hotel owner to make use of this information in a trustworthy and secure manner. In a similar way, the hotel guests also have to trust the underlying systems, which work together with the digital key to function properly. And finally, the hotel guests have to trust that both the hotel owner and the manufacturer have indeed made sure that all necessary security measures have been taken.

However, to speak of a trust relation in a meaningful way, actors have *to be aware* of the fact that they are in a situation where something is at stake. They have to be aware that they are vulnerable and that they depend on other actants. Hotel guests, first and foremost, assess whether the digital key enables them to safeguard their *physical privacy* in the hotel. It is doubtful, however, if hotel guests also take into account the way in which their *informational privacy* is being taken care of when using the digital key. Generally, they do not experience its mediating qualities and the actors–hidden behind the interface–largely operate out of their sight. Consequently, their trust does not extend to what is happening behind the blinking screen of their smartphone.

5 Conclusion

With every step in the innovation process, the hotel key mediates the interaction of the hotel owner and hotel guest in a new manner. Because their relation evolves, the way in which trust is being shaped evolves as well. If we had thought of the key as nothing more than just an instrument to open a door or lock a room, these changes in the trust relation of hotel owner and hotel guest would not have come to the surface.

This article demonstrates that to understand trust relations that are mediated by artefacts, it is necessary to not only focus on the trustor and trustee, but to analyse the specific workings of the artefact involved as well. The *generalized symmetry* as developed by Latour is a fruitful starting point for such an analysis. It addresses the agency of both humans and non-humans and focuses on the networks these actants constitute in order to understand a specific phenomenon such as the forgotten hotel keys central to this article. Especially in the current era, where the ontology of artefacts itself is increasingly becoming networked, this approach is still very up-to-date.

Although analysing the generalized symmetry of both humans and non-humans is necessary to understand trust in the networked era, nevertheless, it is not sufficient. As we saw in the discussion on the family of trust concepts, trust is closely linked to having *positive expectations* about the intentions and actions of others. As these others to a certain extent always remain black boxes, the *perception* we have of them is crucial in developing trust. In the case of the digital key, hotel guests perceive only a limited part of the actants they are actually engaging with. By contrasting the hotel guest's *perception of the digital key* with *the network of actants constituting the digital key*, it becomes apparent where possible trust issues may arise.

Unfortunately, it is beyond the scope of this paper to address the ethical questions that derive from this inquiry. Nevertheless, this paper shows that if one aims at a thorough ethical assessment of practices mediated smart artefacts, an analysis contrasting the experience of the users of the technology with the network of actants brought together by the technology is needed first. Without such an analysis, one runs the risk of missing out what really is at stake in a mediated interaction.

Returning to the family of related trust concepts, it seems that specifically the idea that trust needs *a familiar world* to develop is being stifled by the digital key. Trust can only be established in a world or social context, which to a certain extent is already known by the actors involved. We assume that others perceive the world in a more or less similar way as we do. Our experience of the world inherently contains the inter-subjective constitution of meaning; it is a *coming together of perspectives*.

However, the aim of the digital key app is precisely to circumvent interpersonal interactions and to provide personalized services instead. Moreover, the digital app is constantly reading, interpreting, and anticipating the behaviour of hotel guests. Simultaneously, the hotel guests do not have access to these functionalities and oftentimes are not even aware that they are being interpreted and steered in certain directions. Hotel guests have no way of guessing how they are being read by their digital key (also see Hildebrandt 2013, 19-22, 2015, 183). Consequently, the inter-subjectiveness of the familiar world has to make way for a subjective familiar world.

One way of ensuring that the familiar world no longer is under siege by smart artefacts–as the digital key is certainly not the only app or service currently on the market providing pro-active and personalized services–is to invest in *the ethical design of interfaces*. These interfaces should provide their users with a view on the actants they are actually interacting with. Moreover, these interfaces should be able to represent the use and flow of their users' information in a comprehensible matter.

Research in the domain of philosophy of technology and ethics of technology may contribute to this endeavour by taking interfaces of smart artefacts and how they mediate interactions as their focal point of analysis. What do these interfaces amplify and what do they hide from their users? How does this mediation strengthen or weaken certain values such as autonomy, dignity, and trust? What are ethical design principles that need to be taken to heart? As the digital key is just one example of a much larger technological development, it is not far-fetched to assume that work in this domain will only become more urgent.

As a way of ending this article, I want to refer back to Latour's observation that we should not forget about the artefacts that mediate our interactions. When it comes to the Internet or to Internet-based services, currently there is a lot of attention for large and influential information intermediaries such as Facebook, Apple, and Google. However, we should not forget about the mundane smart artefacts we are carrying around in our pockets and the myriad of actants they bring into our lives, even beyond our awareness.

Acknowledgements

I would like to thank the anonymous reviewers and the editorial board for their constructive comments during the review process.

References

Achterhuis, H. 2001. *American philosophy of technology: The empirical turn.* Bloomington and Indianapolis: Indiana University Press.

Akrich, Madeleine, and Bruno Latour. 1992. "A summary of a convenient vocabulary for the semiotics of human and nonhuman assemblies." In *Shaping technology/building society: Studies in sociotechnical change*, edited by E. Bijker and J. Law, 259-264. Cambridge: The MIT Press.

Ambrosino, B. 2014. "Why the disappearance of hotel room keys marks the end of hospitality." Quartz, accessed 09 June. http://qz.com/177505/why-the-disappearance-of-hotel-room-keys-marks-the-end-of-hospitality/.

ASSA-ABLOY. 2015. "Electronic hotel locking solutions_brochure_English_Nov14.pdf." accessed 9 June. http://www.assaabloyhospitality.com/en/aah/com/press-room/product-documentation/.

Boden, R. 2015. "Apple demonstrates smartwatch keys and payments." NFC World, accessed 10 June. http://www.nfcworld.com/2015/03/09/334534/apple-demonstrates-smartwatch-keys-and-payments/.

Borgesius, F.J. 2014. "Improving privacy protection in the area of behavioural targeting." Dr, Faculty of Law, Instituut voor Informatierecht (IViR), University of Amsterdam.

Brey, P. 2009. "Philosophy of technology meets social constructivism: A shopper's guide." In *Readings in the philosophy of technology*, edited by David M. Kaplan, 98-111. Lanham, Maryland: Rowman & Littlefield Publishers.

Brey, P. 2010. "Philosophy of technology after the empirical turn." *Techné: Research in Philosophy and Technology* 14 (1):36-48.

Brown, C. 2011. "NFC room keys find favour with hotel guests." NFC World, accessed 10 June. http://www.nfcworld.com/2011/06/08/37869/nfc-room-keys-find-favour-with-hotel-guests/.

Chen, Jianqing, and Jan Stallaert. 2014. "An economic analysis of online advertising using behavioral targeting." *Mis Quarterly* 38 (2):429-449.

Ericsson. 2016. Ericsson mobility report. On the pulse of the networked society.

Floridi, L. 2012. "Hyperhistory and the Philosophy of Information Policies." *Philosophy & Technology*:1-3.

Giddens, A. 1991. *Modernity and self-identity, self and society in the late modern age.* Stanford: Stanford University Press.

Giddens, Anthony. 1990. *The consequences of modernity.* Cambridge, UK: Polity Press in association with Basil Blackwell, Oxford, UK.

Giddens, Anthony, and Christopher Pierson. 1998. *Conversations with Anthony Giddens: Making sense of modernity.* Stanford, Calif.: Stanford University Press.

Gomez, Carles, Joaquim Oller, and Josep Paradells. 2012. "Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology." *Sensors* 12 (9):11734-11753.

Gupta, N. 2013. *Inside Bluetooth Low Energy.* Boston/London: Artech House.

Hardin, R. 2006. *Trust.* Cambridge: Polity Press.

Hildebrandt, M. 2013. "Slaves to big data. Or are we? (Esclavos de los macrodatos. ¿O no?)." *IDP. Revista de internet, Derecho Y Política* 17:7-44.

Hildebrandt, M. 2015. "The public(s) onlife. A call for legal protection by design." In *The onlife manifesto. Being human in a hyperconnected era*, edited by L. Floridi, 181-194. Charm: Springer.

Hilton. 2014. "Hilton Revolutionizes Hotel Experience with Digital Check-In, Room Selection and Customization, and Check-Out across 650,000-Plus Rooms at More Than 4,000 Properties Worldwide." accessed 9 June. http://news.hiltonworldwide.com/index.cfm/newsroom/detail/27192.

Ihde, Don. 1990. *Technology and the lifeworld: From garden to earth.* Bloomington: Indiana University Press.

Kaplan, David M. 2009. *Readings in the philosophy of technology.* Lanham: Rowman & Littlefield Publishers.

Kiran, Asle H, and Peter-Paul Verbeek. 2010. "Trusting our selves to technology." *Knowledge, Technology & Policy* 23 (3-4):409-427.

Kohn, Marek. 2008. *Trust: Self-interest and the common good.* Oxford: Oxford University Press.

Kopetz, Hermann. 2011. *Real-time systems. Design principles for distributed embedded applications.* Edited by John A. Stankovic. New York: Springer.

Latour, B. 1992. "Where are the missing masses." In *Shaping Technology/building Society: Studies in Sociotechnical Change*, edited by E. Bijker and J. Law, 225-258. Cambridge: MIT Press.

Latour, Bruno. 1990. "Technology is society made durable." *The Sociological Review* 38 (S1):103-131.

Latour, Bruno. 1993. *We have never been modern.* Harvard: Harvard University Press.

Lindberg, P.J. 2013. "What your hotel knows about you." CNN, accessed 18 June. http://edition.cnn.com/2013/02/26/travel/what-your-hotel-knows/.

Luhmann, N. 1979. *Trust and power. Two works by Niklas Luhmann.* Translated by Howard Davis. New York: John Wiley & sons Ltd.

Luhmann, N. 1988. "Familiarity, confidence, trust: Problems and alternatives." In *Trust: Making and breaking cooperative relations.*, edited by D. Gambetta, 94-107. Blackwell Publishers.

Manley, B. 2015. "Issues loom for keyless entry in hotels." accessed 11 June. http://www.hotelnewsnow.com/Article/15618/Issues-loom-for-keyless-entry-in-hotels.

Mayer-Schönberger, Viktor, and Kenneth Cukier. 2013. *Big data: A revolution that will transform how we live, work, and think.* Boston: Houghton Mifflin Harcourt.

McKnight, D Harrison, Vivek Choudhury, and Charles Kacmar. 2002. "The impact of initial consumer trust on intentions to transact with a web site: A trust building model." *The Journal of Strategic Information Systems* 11 (3):297-323.

McKnight, D.H., and N.L. Chervany. 2002. "What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology." *International Journal of Electronic Commerce* 6:35-60.

Mitchell, R.L. 2006. "It's just the key to your room. Computerworld surveys 100 hotel card keys to explode an urban myth.". Computerworld, accessed 07 June. http://www.computerworld.com/article/2561071/security0/it-s-just-the-key-to-your-room.html.

Möllering, G. 2001. "The nature of trust: From Georg Simmel to a theory of expectation, interpretation and suspension." *Sociology* 35 (2):403-420.

Möllering, G. 2006. *Trust: Reason, routine, reflexivity.* Amsterdam: Elsevier.

Möllering, Guido. 2005. "The Trust/Control duality. An integrative perspective on positive expectations of others." *International sociology* 20 (3):283-305.

Morosan, Cristian, and Agnes DeFranco. 2015. "Disclosing personal information via hotel apps: A privacy calculus perspective." *International Journal of Hospitality Management* 47:120-130. doi: http://dx.doi.org/10.1016/j.ijhm.2015.03.008.

Neuhofer, Barbara, Dimitrios Buhalis, and Adele Ladkin. 2015. "Smart technologies for personalized experiences: A case study in the hospitality domain." *Electronic Markets*:1-12.

Odedra, R. 2015. "Exclusive Q&A: Hilton Worldwide's digital check-in ". HotelierMiddleEast.com, accessed 07 June. http://www.hoteliermiddleeast.com/22579-exclusive-qa-hilton-worldwides-digital-check-in/1/print/.

Pesonen, Juho, and Eric Horster. 2012. "Near field communication technology in tourism." *Tourism Management Perspectives* 4 (0):11-18. doi: http://dx.doi.org/10.1016/j.tmp.2012.04.001.

Pitt, J.C. 2010. "It's not about technology." *Know. Techn. Pol.* 23:445-454.

Schermer, Bart Willem, Bart Custers, and Simone van der Hof. 2014. "The crisis of consent: How stronger legal protection may lead to weaker consent in data protection." *Ethics and Information Technology* 16 (2):171-182.

Seligman, A.B. 1997. *The problem of trust.* Princeton: Princeton University Press.

Sherry, John EH. 1993. *The Laws of Innkeepers: For Hotels, Motels, Restaurants, and Clubs.* Ithaca, New York: Cornell University Press.

Simon, J. 2013. "Trust." In *Oxford Bibliographies in Philosophy*, edited by D. Pritchard. New York: Oxford University Press.

Simpson, Thomas W. 2012. "What is trust?" *Pacific Philosophical Quarterly* 93:550-569.

Taddeo, Mariarosaria. 2009. "Defining Trust and e-trust: From old theories to new problems." *Technology and Human Interaction* 5 (2):23-35. doi: 10.4018/jthi.2009040102.

The-Online-Initiative. 2015. The onlife manifesto. edited by L. Floridi. Cham: Springer.

Thurman, Neil, and Steve Schifferes. 2012. "The future of personalization at news websites: Lessons from a longitudinal study." *Journalism Studies* 13 (5-6):775-790.

van den Berg, B. 2009. "The Situated Self." Doctor, Departement of Philosophy, Erasmus University Rotterdam.

Verbeek, P.-P. 2000. *De daadkracht der dingen.* Amsterdam: Boom.

Verbeek, Peter-Paul. 2011. *Moralizing technology: Understanding and designing the morality of things.* Chicago ; London: The University of Chicago Press.

White, Martha C. 2014. "Skipping the front desk, and checking In with a click." The New York Times, accessed 09 June. http://www.nytimes.com/2014/11/04/business/hotels-test-turning-guests-smartphonoes-into-room-keys-.html?_r=0.

Wittgenstein, L. 2009 [1953]. *Philosophical investigations.* Oxford: Wiley-Blackwell.

Notes

[1] This article is based on, and includes sentences from Keymolen (2016).

[2] Latour never explicitly refers to an actual existing hotel or period of time in which he situates the problem of the missing hotel keys, because it obviously is more a thought experiment than it is an actual empirical case. However, I like to think of it as taking place in the early days of Le Grand Hotel.

[3] It has to be noted that Luhmann and Möllering are not the only trust scholars who focus on these different trust concepts. Most of these notions can be found in the work of other scholars as well. This article will, however, not look further into these different theories. For an overview of conceptualizations of trust in the online environment see Keymolen (2016).

[4] Of course, keycards can also be stolen or forged. Security is never 100%. For example, magnetic stripe keycards can be cloned and there are several tutorials online on "how to hack your hotel keycard."

[5] http://hhonors3.hilton.com/en/promotions/privacy-policy/english.html, accessed on 25 June 2015.

[6] http://hhonors3.hilton.com/en/promotions/privacy-policy/english.html, accessed on 25 June 2015.