scripted

Volume 14, Issue 2, December 2017

Your Smart Coffee Machine Knows What You Did Last Summer: A Legal Analysis of the Limitations of Traditional Privacy of the Home under Dutch Law in the Era of Smart Technology

Lisa van Dongen and Tjerk Timan***

DOI: 10.2966/scrip.140217.208

Abstract

The increasing number of smart devices entering our homes have implications for privacy. Not only do we bring in more spying devices into the home, often these smart objects are linked to data streams or other devices that leave the home – thereby literally taking private matters into public space. In this paper, we take the context of the Netherlands to show that current legal definitions and protections of the home are inadequate to deal with novel privacy threats that stem from devices that interact with us beyond the screen.

Keywords

smart home; privacy of the home; data protection

* Junior researcher and LLM Student at Tilburg University, Tilburg, The Netherlands, l.vandongen@tilburguniversity.edu

** Scientific Policy Advisor at TNO, The Hague, The Netherlands, tjerk.timan@tno.nl

1 Introduction

Today, the Internet has become one of our prime platforms for communication and consumption. Moving beyond the personal computer or smartphones only, increasingly other devices are being connected to the Internet, from coffee machines and watches to beds and toys.[1] Our homes and our activities in the home are thus becoming more and more transparent, due to such objects entering our homes. Through these objects, new forms of spying can be conducted, both qualitatively and quantitatively,[2] that are more invasive than any spying taking place by physically entering and searching the home today.[3] While the rapidly advancing development of the smart(er) home is both undeniably exciting and promising,[4] it is accompanied by a great deal of inadequately answered or otherwise unanswered questions that seem unable to slow its development down enough for us to properly address them.[5] Potential problems arise from many

---

1 Brian Bennet, "Why Smart Coffee Makers are a Dumb but Beautiful Dream" (CNET, 14 November 2015) available at https://www.cnet.com/news/why-smart-coffee-makers-are-a-dumb-but-beautiful-dream/ (accessed 17 March 2017); 22 CityLink, "The Internet of Things is Here: Fitness Wearables, Smartwatches & Smartglasses" (5 August 2016) available at https://22citylink.com/future-internet-of-things-fitness-wearables-smartwatches-smartglasses/ (accessed 19 March 2017); Ashley Carman, "Sleep Number's New 360 Smart Bed Automatically Adjusts to Your Sleep Position" (The Verge, 8 January 2017) available at http://www.theverge.com/circuitbreaker/2017/1/8/14195396/sleep-number-360-smart-bed-ces (accessed 19 March 2017); Emmeline Taylor and Katina Micheal, "Smart Toys that are the Stuff of Nightmares" (2016) 35(1) IEEE Technology and Society Magazine 8-10.

2 Tamara Denning, Tadayoshi Kohno and Henry Levy, "Computer Security and the Modern Home" (2013) 56(1) Communications of the ACM 94-103, p. 95; Saadi Lahlou, Marc Langheinrich and Carsten Röcker, "Privacy and Trust Issues with Invisible Computers" (2005) 48(3) Communications of the ACM 59-60.

3 See, for example, the dissenting opinion of Justice Louis Brandeis in *Olmstead v United States*, 277 U.S. 438 (1928); Bert-Jaap Koops, Hanneke van Schooten and Merel Prinsen, "Recht naar Binnen Kijken: Een Toekomstverkenning van Huisrecht, Lichamelijke Integriteit en Nieuwe Opsporingstechnieken" (2004) SDU Uitgevers 59-64.

4 See, for instance, Jürgen Bohn et al., "Living in a Word of Smart Everyday Objects – Social, Economic, and Ethical Implications" (2004) 10(5) Human and Ecological Risk Assessment 763-785.

5 See, for instance, Bert-Jaap Koops, "Digitaal Huisrecht" (2017) 23 Nederlands Juristenblad 183-187; Donghee Shin, "A Socio-Technical Framework for Internet-of-Things Design: A Human-Centered Design for the Internet of Things" (2014) 31 Telematics and Informatics

uncertainties regarding these technologies. For instance, where do the digital perimeters of the protected home end?[6] How will privacy be protected, and from whom? Or, in light of the rise of autonomous technological objects, should we start asking from what? Even though it is not possible to properly address and find an answer to these questions in the limited size of this paper, if at all at the present time, these questions are important to raise and consider for the protection of privacy in an increasingly smart(er) world".

Instead, this paper will address the question: are the existing definitions of privacy of the home adequate to deal with today's challenges posed by 'smart home' technologies? The focus of this analysis will be on the legal landscape of the Netherlands. As will be argued throughout this paper, this question is answered in the negative. To demonstrate that some of the privacy-related problems are more pressing than most people seem to realise, this paper will first elaborate on developments and implications of smart technologies for the home environment in the second section. This will be followed by a breakdown of some of the elements of the Dutch "home right" in the third section of this paper, for which the focus will be on the meaning and ramifications of the limited legal definitions used for both the "home" and "entering". In addition, the potential and limits of data protection to account for these weaknesses will be explored in the fourth section. Furthermore, two smart objects will be analysed in the fifth

519-531; Gloria Fuster and Amandine Scherrer, "Big Data and Smart Devices and Their Impact on Privacy" (European Parliament, 2015) available at http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL_STU(2015)536455_EN.pdf (accessed 17 March 2017).

6 Bert-Jaap Koops and Merel Prinsen, "Glazen Woning, Transparant Lichaam. Een Toekomstblik op Huisrecht en Lichamelijke Integriteit" (2015) 80(12) Nederlands Juristenblad 624-230, p. 627; Albert Meijers, "Overheidsverantwoordelijkheid in het Informatietijdperk: Een Pleidooi voor het Creëren van Genormeerde Experimenteerruimte" in Dennis Broeders, Colette Cuijpers and Corien Prins (eds.), *De Staat van Informatie* (Wetenschappelijke Raad voor het Regeringsbeleid: Amsterdam University Press, 2011), pp. 113-114.

section, namely the smart thermostat and the smart toy 'Hello Barbie'. These analyses will be used to illustrate the weaknesses under the existing scope of data protection and the "home right".

This paper aims to convey two messages. First, that the traditional understanding of privacy of the home in the Netherlands is in need of reconsideration in the era of smart technology. Second, that the ramifications of smart technologies in the home environment require a (stronger) protection of privacy, not just against the state, but increasingly also in horizontal relations.

2 The smart home: what's new?

2.1 Old problem?

People already have experience with the information flow and the increasing speed and accessibility of the Internet, so the data processing conducted by smart technology does not seem like something new.[7] However, the magnitude of the information flow has increased significantly and is omnipresent, and only increases due to the rapid speed at which smart technology makes it into our homes and lives. Smart objects can act autonomously, interact and share information with networks, amongst "themselves" and with the entities at the other end of the processes,[8] and to some degree even control the decisions made by the human operator.[9] In addition, most of these smart objects are not

---

7 Carsten Röcker, "Social and Technological Concerns Associated with the Usage of Ubiquitous Computing Technologies" (2010) 11(1) Issues in Information Systems 61-68.

8 Denning, Kohno and Levy, "Computer Security", *supra* n. 2; Alan Davy, "Components of a Smart Device and Smart Device Interactions" (M-Zones White Paper, 2003).

9 The design of smart objects often does not allow for human operators to control the vast majority of settings, if at all. Even if such objects (often without screen) provide for some degree of control, it is still unlikely that the human operator will inter alia due to the "script" of such technology and the competence necessary for a human operator to do so. See, for instance, Madeleine Akrich, "The description of technical objects" (1992) in Wiebe Bijker and John Law (eds.), *Shaping Technology/Building Society: Studies in Sociotechnical Change*

perceived as the largely autonomous computers that they are because of their design.

> 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.[10]

Moreover, the line between offline and online has been blurred by the interaction and interconnectedness of smart objects with environments, since a smart object is no longer limited only to 'online use'.[11] The significant changes in the socio-political order brought on by smart technology are not mere side effects; it is the objective of smart technology and the Internet of Things to transform the world.[12] As will be elaborated on further below, the development of the Internet of Things and smart(er) homes also puts pressure on the traditional relationship between public and private entities, and has ramifications for the autonomy and privacy of the human operator.

While one could think of areas or situations in which such consequences could be justified, there are also places and situations in which this proves more problematic. One such place is the home, arguably the most important physical place for an individual's privacy. For instance, a common and plausible assumption is that a breach of privacy of the home often entails the breach of

(Cambridge, MA: MIT Press); Debra Howcroft, Natalie Mitev and Melanie Wilson, "What we may learn from the social shaping of technology approach" in John Mingers and Leslie Willcocks (eds.), *Social theory and philosophy for information systems* (Chichester: Wiley, 2004) 329–371.

10 *Supra* n. 7, p. 62.

11 Friedemann Mattern, "The Vision and Technical Foundations of Ubiquitous Computing" (2002) 2(5) *Upgrade* pp. 2-6; Friedemann Mattern, "Vom Verschwinden des Computers – Die Vision des Ubiquitous Computing" in Friedemann Mattern (ed.), *Total vernetzt* (Heidelberg: Springer-Verlag, 2002), pp. 1-41.

12 *Supra* n. 7, p. 61.

another type of privacy as well.[13] There are potentially many privacy-related issues connected to an Internet of Things. The context of the home is arguably the most prominent example, or at least the most visible place where an Internet of Things might materialise. The home as a classical bastion of privacy protection presents a crucial stage for projecting and testing novel privacy issues that might result from this smartness entering. While the behaviour or personal communications of an individual are objects of privacy protection in separate parts of the law, they are also largely covered by the protection of privacy of the home.[14]

A first concern with privacy of the home is the reasonable expectation of privacy one may have in his or her home. The negative right to protection of privacy of the home will be in jeopardy not only because smart devices in the home record activities in places that were formerly unrecorded, but also due to the ease with which this recorded data can travel amongst these devices. Moreover, some of these smart objects (for instance, a smartphone) regularly leave the home,[15] or external storage services are used (such as cloud storage of personal files), which affects the distinction between inside and outside the home. This means that breaching the privacy of the home often also affects other types of privacy relevant for the human operator in the Internet of Things, bringing us full circle.

Secondly, smart objects that have made into our homes use a myriad of ways of transmitting and/or storing information, making it easier and more worthwhile to listen and look into the information going back and forth between

---

13 For instance, the home is an overarching spatial privacy comprising other types of privacy such as behavioural, intellectual and communicational privacy. Bert-Jaap Koops et al., "A Typology of Privacy" (2016) 38 University of Pennsylvania Journal of International Law 483-715, p. 570.

14 *Ibid.*, pp. 528, 514-520, 570.

15 Denning, Kohno and Levy, "Computer Security", *supra* n. 2, p. 94.

smart objects, the network they are in, and places outside the home connected to with computing-embedded objects inside the home and external actors.[16]

Third, it is also necessary to observe that there are often multiple residents in a home that share spaces and devices in the home. According to Denning, Kohno and Levy, the smart home also presents a more dangerous home with its private and semi-private spaces, because:

> [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.[17]

Smart home technologies allow for a lot of information going back and forth on all residents between their home and several external service providers. In this context, one could also wonder whether there is also additional spatial privacy between residents' bedrooms within the right to privacy of the home. Should the smart scale in one bedroom and the closet in another be allowed to share information they have obtained, even within the home? Moreover, information will inevitably also be collected on any visitor. Even if people choose not to bring any smart objects into their own home, they will increasingly be confronted with such objects, and ultimately cannot help that data will be collected on them, too.[18]

Consequently, the rise of smart technology is not a case of merely replacing the old with the new, and we must not treat it as such.[19]

---

16 Koops, van Schooten and Prinsen, "Recht naar Binnen Kijken", *supra* n. 3, pp. 58-59.

17 Denning, Kohno and Levy, "Computer Security", *supra* n. 2, p. 96.

18 *Supra* n. 7, p. 63.

19 Bert-Jaap Koops, "Digitale Grondrechten en de Staatscommissie: Op Zoek naar de Kern" (2011) 2(2) Tijdschrift voor Constitutioneel Recht 168-185, p. 185.

2.2 State versus/and the private industry

Discussions on threats to the privacy of the home often revolve around technological objects such as tele-lenses and high-quality miniature cameras, and the search of personal computers, etc., rather than around possible usages of smart household appliances.[20] This is understandable since these types of technologies are the first to come to mind if the "home right" is approached merely in the context of the government-individual relationship. This is actually one of the challenges of privacy in the "smarter world". Most of the attention in the Netherlands regarding this right goes to the vertical effect of privacy protection, while it is the private sector who is mostly responsible for all the smart technology capable of being used as spy equipment making it into our homes. The vertical effect here refers to protection of the individual's privacy against the state, often in the context of surveillance or criminal investigations. Although protection of the individual against the state is obviously not of less importance, the industries can continue to do business as usual, while they (and tech savvy individuals) are able to commence large-scale two-tiered information transactions.[21] This possibly complicates the relationship between governments and the private industries, as we have seen in a recent *FBI v Apple* case in the United States.[22] In this case, the Federal Bureau of Investigation (FBI) had first attempted to gain access to information by making Apple Inc. "hack" an iPhone.[23]

---

[20] Koops, van Schooten and Prinsen, "Recht naar Binnen Kijken", *supra* n. 3, p. 28.

[21] Eliza Mik, "The Erosion of Autonomy in Online Consumer Transactions" (2016) 8(1) Law, Innovation and Technology 1-38, pp. 12-14, 37; Irina Manta and David Olson, "Hello Barbie: First They Will Monitor You, then They Will Discriminate Against You. Perfectly" (2015) 67(1) Alabama Law Review 134-187, pp. 136-139.

[22] Bruce Schneier, "Why You Should Side with Apple, Not with the FBI, in the San Bernardino iPhone Case" (The Washington Post, 18 February 2016) available at http://www.washingtonpost.com/posteverything/wp/2016/02/18/why-you-should-side-with-apple-not-the-fbi-in-the-san-bernardino-iphone-case/ (accessed 13 July 2017).

[23] Arjun Kharpal, "Apple vs FBI: All You Need to Know" (CNBC London, 29 March 2016) available at http://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html

When the latter refused and a legal battle commenced,[24] the FBI supposedly turned to an unidentified third party to find flaws in the iPhone's system, and to obtain software that enabled the FBI to hack the iPhone.[25] The legal battle that emerged between Apple Inc. and the FBI was of particular interest, because the ongoing trend of increased surveillance certainly puts the relationship between the private industry and the government under pressure.[26] In the Internet of Things, the private industry holds a very powerful position in comparison to the state. However, some governments are clearly finding tools of their own to obtain access. Where this case revolved around gaining access to a smartphone, one can imagine similar interest by the state to access information collected by commercial smart devices in the home. It would, therefore, make sense to re-evaluate the relationship between the state and private industries, to see how much the private industry facilitates, or is to facilitate and possibly even contribute directly to the possible breach of, what is in fact, a human right.[27] The right to privacy may not be absolute, but the establishment of limitations to a human right as clearly and as up-to-date as possible is certainly essential for its effectiveness.[28]

(accessed 17 March 2017); David Pierson, "FBI vs. Apple: How Both Sides were Winners and Losers" (Los Angeles Times, 29 March 2016) available at http://www.latimes.com/business/technology/la-fi-tn-apple-fbi-explainer-20160329-snap-htmlstory.html (accessed 17 March 2017); Arash Khamooshi, "Breaking Down Apple's iPhone Fight with the U.S. Government" (New York Times, 21 March 2016) http://www.nytimes.com/interactive/2016/03/03/technology/apple-iphone-fbi-fight-explained.html (accessed 17 March 2017).

24 Tim Cook, "A Message to Our Customers" (Apple, 16 February 2016) http://www.apple.com/customer-letter/ (accessed 19 March 2017); Pierson, "FBI vs. Apple", *supra* n. 23.

25 Kharpal, "Apple vs FBI: All You Need to Know", *supra* n. 23.

26 Pierson, "FBI vs. Apple", *supra* n. 23; Khamooshi, "Breaking Down Apple's iPhone Fight", *supra* n. 23.

27 See, for instance, Bruce Schneier, "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World" (New York: W.W. Norton & Company, 2015).

28 Sanne Buisman and Sandra Kierkels, Commentaar op Artikel 12 van de Grondwet' in Ernst M. Hirsh Ballin and Gert-Jan Leenknegt (eds), *Artikelsgewijs commentaar op de Grondwet* (Web

2.3 Transparency, awareness and consent

It was argued in the former section that with the coming of an Internet of Things, there are considerable new risks and uncertainties when it comes to privacy protection in the home. However, returning to legal reality, we have to ask ourselves how and to what extend these new technologies truly lead to such considerable changes that legal frameworks are starting to fail, or that we are crying wolf? Many privacy scholars would advocate the former, stating that arguably "technological entering of the home" would be a more intrusive breach than physically entering,[29] for it is harder – if possible at all – for the individual to discern that his or her rights are being breached.[30] Röcker adds that technology is becoming more and more sophisticated, leading to a situation in which 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.[31] Where one might argue that a direct entering of the home might be experienced as more intrusive to the "home right" because it entails a direct confrontation, at least the residents in the case of physical entrance (often) know when their home was invaded and to some extent the individuals will be able to follow the actions of the intruders – they may even be able to contest or fight the intrusion (for instance the possibility, however small, to obtain "justice" in retrospect). The other side of this spectrum, being monitored from the outside via one's data, presents a maybe less direct, but more severe intrusion on one's

edition, 2016) available at http://www.nederlandrechtsstaat.nl (accessed 17 March 2017) pp. 7-9.

29 Paul Mevis, "De Bescherming van de Woning 25 Jaar Later" in Ebby Hofstee et al. (eds.), *Kringgedachten. Opstellen van de Kring Corstens* (Deventer: Kluwer, 2014), pp. 160-161.

30 Koops and Prinsen, "Glazen Woning", *supra* n. 6, p. 627.

31 *Supra* n. 7, pp. 61, 64.

feeling of privacy. The realisation that you *may* be watched adds to the overall distrust that could be caused by the increasingly smart(er) environment and the feeling of losing control in or over this environment.[32] This sense of distrust, or perhaps even paranoia, may also affect people's behaviour,[33] even inside their own home, rendering the protection of the personal freedom pursued by the "home right" ineffective in practice.[34] This is called the chilling effect[35] and this effect has actually been measured in a recent study regarding internet spying.[36]

We argue here that a reasonable expectation of privacy inside the home should remain, even if the services of third parties that might reside outside the home are being used. To exemplify, our communication infrastructure has changed significantly over the past decade or so, which has led to very different patterns of social interaction and communication and it has significantly changed the way in which individuals handle their (personal) information.[37] The overall emerging practice to entrust third parties with personal information, mostly to make sure they can access it elsewhere and always, and to ensure that they do not lose the information, has developed as a key element of the present-day mobility of both the individual and their information. Admittedly, trusting

---

32 Kerstin von Locquenghien, "On the Potential Social Impact of RFID-Containing Everyday Objects" (2006) 2(1) Technology & Innovation Studies 57-78; *Supra* n. 7, pp. 62, 64; Lahlou, Langheinrich and Röcker, "Privacy and Trust Issues", *supra* n. 2, p. 60.

33 *Supra* n. 13; Maša Galič, Tjerk Timan and Bert-Jaap Koops, "Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation" (2017) 30(1). Philosophy & Technology 9-38 (for an overview of Bentham's and Foucault's theories on surveillance).

34 Neil Richards and Woodrow Hartzog, "Taking Trust Seriously in Privacy Law" (2016) 19 Stanford Technology Law Review 431-473, pp. 431, 435; *Supra* n. 7, pp. 61, 64; Koops and Prinsen, "Glazen Woning", *supra* n. 30.

35 See, for instance, David Lyon, "A Surveillance Winter: The Chilling Effect on Freedom" (The Whig, 22 January 2015) available at http://www.thewhig.com/2015/01/22/a-surveillance-winter-the-chilling-effect-on-freedom (accessed 22 July 2017).

36 See John Penney, "Chilling Effects: Online Surveillance and Wikipedia Use" (2016) 31(1) Berkeley Technology Law Journal 117-173.

37 Bert-Jaap Koops, 'Digitale Grondrechten en de Staatscommissie: Op Zoek naar de Kern' (2011) 2(2) Tijdschrift voor constitutioneel recht 168-186, pp. 176-177.

Google as a safe-keeper of personal information may indeed affect the reasonable expectation of privacy negatively in this context,[38] but the mere use of third-party services in itself should not necessarily have this negative effect. The mobility of individuals and of information is essential to the success of the *smart* society, yet there is still a lot to be said about the varying trustworthiness of third parties as actors in this society.[39] New technologies and services are not just a digitised or updated versions of what once was; they are technological developments capable of bringing on significant changes in society in both behaviour and communication.[40] The sentient home might be one of them – this should however not affect the reasonable expectation of privacy an individual can have in the home. Even though many individuals may have been alarmed by stories about the use of smart technologies, or merely had their reservations, the realisation that the combination of data-handling processes of smart objects increase the "transparency" of our home has not yet found its way to the public at large.[41]

This also applies to the information given prior to letting technologies into our house and/or providing them with access to information: how informed is this consent, really?[42] Has the obtaining of consent been reduced to a mere formality of good form? Does bringing a smart object into your home equal a general consent to enter the home? Naturally, there are limitations imposed upon both public and private parties when it comes to invading the privacy of the home, both by data protection and privacy regulations. However, the extent to

---

38 *Ibid*., p. 171; Mik, "The Erosion of Autonomy", *supra* n. 21, pp. 28, 39.

39 *Ibid*., p. 177.

40 *Supra* n.7, pp. 61, 63-64; *Supra* n. 37, p. 185; *Supra* n. 4, p. 764.

41 Colette Cuijpers and Bert-Jaap Koops, "Smart Metering and Privacy in Europe: Lessons from the Dutch Case" in Serge Gutwirth et al. (eds.), *European Data Protection: Coming of Age* (Dordrecht: Springer Netherlands, 2013) p. 292.

42 See, for instance, Roger Brownsword, "Autonomy, Delegation, and Responsibility: Agents in Autonomic Computing Environments" in Mireille Hildebrandt and Antoinette Rouvroy (eds.), *Law, Human Agency and Autonomic Computing* (Oxon: Routledge, 2011), p. 68.

which this protection remains adequate leaves much to desire, as will be further explored in the fourth and fifth sections.

3 Breakdown of privacy of the home: Article 12 of the Dutch Constitution

3.1 Legal definition of 'home'

In the Netherlands, Article 12 of the Dutch Constitution contains the "home right", which covers the protection against government infringements of the home, without permission of the residents when none of the exceptions to this right are applicable. It can be classified as a form of spatial privacy since it entails the right to include and exclude people from a private place for privacy considerations. This Article is actually a *lex specialis* from Article 10, which entails the constitutional right to personal life.[43] Under Dutch law and existing case law, the home found in Article 12 of the Dutch Constitution is described as a physical space that is recognisable as a home (although this can entail a house, a boat or even a tent or a room), which is both meant and arranged in a manner as to accommodate a person or a limited number of people in a household setting in pursuing a private life cut off from the outside world.[44] Interestingly, Dutch case law has initially provided for the abolishment of the requirement that the people living in a place meeting the criteria should do so legally, which means that illegal inhabitants of a home are also entitled to protection under Article 12 of the Dutch Constitution.[45] The essence of this right is that it acknowledges the need

43 *Supra* n. 28, p. 1

44 *Supra* n. 28, p. 4; Kamerstukken I 1997/98, 25 442, No. 231b, 2 (Senate of The Netherlands).

45 *Supra* n.28, pp.12-13; Koops, van Schooten and Prinsen, "Recht naar Binnen Kijken", *supra* n. 3, p. 30.

for the individual to have a place where one can be him or herself, completely, without interference or intrusion from the outside world.[46]

It is apparent that some elements of the Dutch definition of the home, such as the prerequisite that there is a household setting and that the home should be recognisable as such, seem to preclude a broader scope as to include spaces such as an office. The Dutch definition of the home has proven to be outdated since *Niemietz v Germany*,[47] in which the Strasbourg Court found that professional life and the office may also be covered by Article 8 of the European Convention on Human Rights (ECHR).[48] Consequently, proceedings brought before the court in the Netherlands based on privacy of the home require Article 8 of the European Convention on Human Rights when it involves the workplace or the professional life, and cannot be based on Dutch law.[49] The Strasbourg Court argued that the distinction cannot always be made between professional and personal life due to an overlap between the two. One line of reasoning is that the "right to respect for personal and family life" of Article 8 of the ECHR also includes the possibility for individuals to develop relationships.[50] Since a large part of our lives is spent in the workplace, many social relations are formed there. Another factor could be the type of activities that are connected to a particular type of work, since some

---

46 Antonius Tak, "Het Huisrecht" (Dissertation, Hoenderloo, 1973) pp. 9-10; Koops, van Schooten and Prinsen, "Recht naar Binnen Kijken", *supra* n. 3, p. 28; *Supra* n. 13, pp. 59, 70-71. This definition goes well beyond the category of proprietary privacy, which is connected, and limited to, to physical property of the home by itself.

47 Niemietz v Germany (1992) 116 EHRR 97.

48 Koops, van Schooten and Prinsen, "Recht naar Binnen Kijken", *supra* n. 3, p. 30; *Supra* n. 28, p. 5; Ursula Kilkelly, "The Right to Respect for Private and Family Life: A guide to the implementation of Article 8 of the European convention on Human Rights" (Council of Europe, August 2003) available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168007ff47 (accessed 17 March 2017), p. 19.

49 Koops, van Schooten and Prinsen, "Recht naar Binnen Kijken", *supra* n. 3, p. 16; *Supra* n. 28, p. 5.

50 Kilkelly, "The Right to Respect for Private and Family Life" *supra n*. 48, p. 11.

professions may complicate the making of this distinction by their very nature.[51] It is likely that this distinction will only become more difficult to make with the increasing presence of smart objects in the home, since more and more processes will be controllable and discernible from both inside and outside the home. This may ultimately change the function of the home, because the individual will be able to conduct activities from both inside and outside the home, regardless of whether they are of a personal nature or work-related.[52]

The general right to privacy under Article 10 of the Dutch Constitution does provide for some level of protection in this context, but the protection offered in this Article will arguably be inadequate to cover breaches or harms of spatial privacy. This has to do with both the core of the "home right" and the autonomy of the individual. Autonomy is one of the basic elements of privacy, as it refers to the control an individual has over his or her own person, to his or her personal life and even to the control over information on him or her in "absence of (objectionable) external influences in the context of action".[53] Even if its effectiveness has been compromised by the current practice, the core of the "home right" obviously goes a lot further than that insofar as to, theoretically, even entail the *inviolability* of the home. Some legal scholars have argued that the wording of Article 12 of the Dutch Constitution should be changed to include the inviolability of the home to better capture the core of this right.[54] Autonomy is seen as a key element to feeling safe from the outside world because it provides the individual with control over his or her own home.[55]

---

51 Koops, van Schooten and Prinsen, "Recht naar Binnen Kijken", *supra* n. 3, p. 30; Kilkelly, "The Right to Respect for Private and Family Life" *supra n*. 48, pp. 19, 65.

52 Koops and Prinsen, "Glazen Woning", *supra* n. 6, p. 626.

53 Brownsword, "Autonomy, Delegation, and Responsibility", *supra* n. 42, pp. 68-69; Koops, van Schooten and Prinsen, "Recht naar Binnen Kijken", *supra* n. 3, pp. 28, 33.

54 Koops and Prinsen, "Glazen Woning", *supra* n. 6, p. 627.

55 Koops, van Schooten and Prinsen, "Recht naar Binnen Kijken", *supra* n. 3, p. 28.

3.2 Definition of entering

The limited definition of intrusion in Article 12 of the Dutch Constitution is another factor demonstrating that privacy of the home in the Netherlands is not ready for the digitised and the digital home.[56] Some legal scholars have argued that some of the definitions used in this article are in need of reconsideration,[57] some say the article itself is in need of revision if it wants to be able to address today's and tomorrow's challenges.[58] Yet others have stated that the wording of this Article does not really constitute the protection of a right within this meaning to begin with. For instance, Mevis argues that the way this right has been implemented and applied in practice has emphasised the element of *entering* the home, meaning the article merely entails the right to protection from non-residents entering the home without consent of the residents, more specifically against state officials.[59] There is something to say for the latter point of view, since this law mainly applies to cases in which this right is breached by physically crossing (even if just partially) imaginary or physical boundaries of the home. The Dutch court came to this conclusion in a case revolving around the question whether a government official sticking his arm through an open door constituted a breach of the "home right".[60] The concept of entering is thus defined as a human act, but this seems to exclude the situation that equipment is used with the objective to avoid breaching the "home right" by entering physically.[61] This

---

56 *Supra* n. 28, pp. 1-2; Koops and Prinsen, "Glazen Woning", *supra* n. 6, p. 624; *Supra* n. 19, pp. 168, 181-183.

57 See, for instance, Albert Meijers, "Overheidsverantwoordelijkheid in het Informatietijdperk", *supra* n. 6, p.113.

58 Koops and Prinsen, "Glazen Woning", *supra* n. 6, p. 627.

59 *Supra* n. 29, p. 158.

60 The answer was yes. See 'Arm case', 1956 as cited in *supra* n .28, p. 2; Koops, van Schooten and Prinsen, "Recht naar Binnen Kijken", *supra* n. 3, p. 31.

61 Koops and Prinsen, "Glazen Woning", *supra* n. 6 p. 626; Koops, van Schooten and Prinsen, "Recht naar Binnen Kijken", *supra* n. 3, p. 32.

would mean that autonomous technology used inside or outside the home to obtain information inside the home will not qualify and therefore there is no protection under the "home right" for this practice.[62]

Another issue in this respect is the capability of the Dutch "home right" to affect the rights of private individuals in their relationships with other private parties. Although the horizontal effect of privacy of the home has been acknowledged in Dutch case law, it is very limited.[63] Privacy of the home in Dutch law and practice mostly aims to protect individuals from state intrusion. This can also be inferred from privacy-related regulations, since they focus mostly on the state entering the home in the context of surveillance, criminal investigations and for administrative purposes.[64] This renders the potential horizontal effect questionable in the Dutch legal system.[65] In comparison, the horizontal effect of Article 8 of the ECHR has been widely acknowledged, even though it was originally designed to protect individuals against a state.[66] Interestingly, in the European legal framework on personal information, both individuals and the private industry are addressed alongside the government of the Member States. Moreover, the question of where information is localised matters more for the applicability of Dutch law than it does for European (Union) law. Consequently, non-domestic legal frameworks seem more equipped to

---

62 *Supra* n. 28, p. 2.

63 For completeness, it must be said that data protection has been left out of the equation here. Data protection is also important for privacy protection, but will not be elaborated on until the sixth section for reasons explained there.

64 E.g. 'Wetboek van Strafvordering', 'Algemene Wet op het Binnentreden'. The Dutch Data Protection Act ('Wet Bescherming Persoonsgegevens') is an exception, since it is not limited to protection against the state.

65 See case NJ 2000/152 (Hof Amsterdam, 8 January 1998) and case NJ 2013/153 (Hoge Raad, 28 October 2011) as cited in *supra* n. 28, p. 12.

66 Juliane Kokott and Christoph Sobotta, "The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR" 3(4) (2013) International Data Privacy Law 222-228, pp. 225-226; *Supra* n. 19, p. 171.

address privacy-related problems arising from the digitised home, for at least they are not necessarily limited to physical entering by state officials for finding a breach of the individual's right to privacy of the home. However, many new technologies have the ability – or are specifically designed – to enter the home.

4 Data protection to the rescue?

With the rapidly increasing information flow, a lot of attention had been paid to data protection, not just by national governments, but also by the Strasbourg Court and European Union (EU) institutions.[67] This is a very significant and promising development, but there are important differences between the protection of privacy and of data that beg caution with putting our faith solely or too much in the latter. The legal relevance of the differences is also apparent from the way EU Member States have regulated the protection of personal data: often as a separate paragraph or article to privacy.[68] As a positive development in data protection, it is found to have horizontal effect and hold obligations for private parties.[69] As argued previously, the horizontal effect of privacy protection in the Netherlands is still quite limited, as legislation based on or related to the Articles in the Dutch Constitution on privacy is focused mostly on surveillance by the state, criminal investigations and public administration. The horizontal effect of the Dutch Data Protection Act has been important progress.

However, as both secondary legislation on data protection in the EU and the Dutch Data Protection Act describe, data protection laws only provide protection against the processing of personal identifiable information and is thus both much more limited than privacy protection, and more encompassing. This

---

[67] *Ibid.*

[68] Supra n. 13, pp. 44-45.

[69] Kokott and Sobotta, "The Distinction between Privacy and Data Protection" (2013) *supra* n. 66, p. 225.

can be explained as follows. Some personal information can fall outside the scope of privacy protection because it does not relate to or interfere with the private life, but could still fall within the scope of data protection if it identifies, or is capable of identifying, an individual, and any type of processing thereof is or has taken place.[70] This is a scenario in which data protection compliments privacy protection.

However, the opposite situation can also present itself. It is possible that data on individuals is being processed according to the legal requirements for the processing of personal data, but is, nevertheless, interfering with the private life.[71] Data protection does not cover all the information about an individual's exercise of his or her privacy. To consider the magnitude of data being collected on each individual every day is important,[72] especially since this scenario is hardly uncommon in the era of smart technology. Unfortunately, data protection may in some cases not prohibit the processing, whereas privacy would require a justification.[73] Therefore, we cannot afford to focus too much on data protection alone. Privacy protection will remain vital to protect the interests of individuals, and will thus have to adapt as well to the developments in smart technology and society.

In this context, it is also noteworthy that the essence of the protection of data and privacy is also not the same. While the protection of data is imperative for privacy protection in an increasingly smarter world, the most important requirement is that the data is capable of identifying a specific individual,

---

70 See, for example, Segerstedt-Wiberg and Others v Sweden App no. 62332/00, ECHR 2006-VII, paras. 88-90.

71 Amann v Switzerland App no. 27798/95, ECHR 2000-II, paras. 69ff and 80; Rotaru v Romania App no 28341/95, ECHR 2000-V, para. 46; Kokott and Sobotta, "The Distinction between Privacy and Data Protection" (2013) *supra* n. 69.

72 M.M. v UK App no. 24029/07 (2012), para. 200.

73 Amann, paras. 69ff and 80; Rotaru, para. 46.

whereas privacy aims to protect the individual's ability to just be without having to fear (unforeseeable, disproportional and/or unjustified) interference. One may wonder why this is important if a person may not be identified by some of the information collected, but this brings us back to the panopticon and the mechanisms of surveillance: the mere possibility that everything individuals do or say inside their home is being watched would be a severe interference of the private home-life in itself. Data protection will not suffice as a substitute for this type of privacy by a long shot. The "home right" touches upon parts of an individual's identity and the overall feeling of being safe inside the home from the outside world to just "be", which is much broader than just the identifiable information about it.[74]

To illustrate the shortcomings of data protection, the next section constitutes two case assessments of two smart objects and the ways they touch upon privacy and data protection in horizontal relations. The legal definitions previously discussed of Article 12 of the Dutch Constitution will not be discussed here, since it has already been established that they only provide protection against a limited type of intrusions of privacy of the home conducted mostly by the state.

5 Illustration: The case of the smart thermostat and toy

The question of how and to what extent trends and phenomena such as cyberspace, Internet of Things, semantic web, or industry 4.0 have such an effect on society and daily life that legal systems need to change accordingly, has raised many discussions among legal scholars since roughly the 1990s[75]. In the absence

---

[74] Tak, "Het Huisrecht" *supra* n. 46, pp. 9-10; Koops, van Schooten and Prinsen, "Recht naar Binnen Kijken", *supra* n. 3, p. 28; *Supra* n. 13, pp. 59, 70-71.

[75] Not aiming to repeat this discussion to its full extent, see for the start of this debate and the main argument: Lawrence Lessig, "The law of the Horse: What Cyberlaw Might Teach" (1999) 113(2) Harvard Law Review 501-549.

of a clear test of the level of influence technologies have on legal systems, the issues caused by smart technologies entering the home as raised in this article can be critiqued, or scrutinised according to similar lines that are posed in the debate on the existence of such a thing as Information and Communications Technology (ICT) law. One of the main contestations is that the legal systems should be based on – and informed by – principles rather than day-to-day cases and situations informing legal systems. However, it can be argued that technological changes as we are experiencing in the present day do in fact alter daily life to such an extent that legal principles start breaking down. One of such areas where this is argued to be happening, is privacy.[76] As explained in previous sections, especially the home as private place, as a place to truly be oneself, is under threat due to novel "smart" technologies that enter the home. Two such examples below show how and to what extend privacy is under threat and how and to what extent data protection plays a role in protecting privacy in – and of the home.

5.1 The smart thermostat

5.1.1 Functions and privacy settings

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.[77] Furthermore, it can help determine which devices

---

[76] See, for instance, Mireille Hildebrandt and Bert-Jaap Koops, "The Challenges of Ambient Law and Legal Protection in the Profiling Era" (2010) 73(3) The Modern Law Review 428-460.

[77] See Eneco, "Slim huis met Toon"(n.d.) available at https://www.eneco.nl/toon-thermostaat/slim-huis-met-toon/ (accessed 22 July 2017).

inside the home are the least "friendly" to the overall usage and costs of your energy consumption. The smart thermostat requires a WiFi connection, and needs to be linked to the reader of the gas or electricity meter 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.[78]

"Toon" as a particular smart thermostat is mostly part of a service contract, for which the privacy statement says that the necessary personal information can be retrieved, processed and stored,[79] but nothing is said about their direct access to information situated on the thermostat. For an 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.[80]

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 consent hereto. 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

---

78 *Ibid*.

79 Eneco, "Privacyverklaring Toon® van Eneco" (2016) available at http://www.eneco.nl/-/media/eneco/pdf/voorwaarden-en-brochures/voorwaarden-overig/enecotoonprivacyverklaring.ashx?la=nl-nl (accessed 20 July 2017).

80 Eneco Consumenten B.V., "Voorwaarden voor de Toon® App van Eneco" (2015) available at http://www.eneco.nl/-/media/eneco/pdf/actie/voorwaardentoonoptablet.ashx?la=nl-nl (accessed 20 July 2017).

provided by the thermostat, namely the smart fire alarm, hue smart lamps, solar panels, and smart plugs.[81] These limitations are satisfactory from a privacy perspective, one could argue: the smart thermostat allows the end-user to tweak the settings, no personal data is being collected unnecessarily and in the end, more insight can be gained on electricity use, leading to potential benefits in terms of energy saving.

5.1.2 Privacy and data protection

The object of this analysis is not just situated in the home, but is also capable of partially running it. Such an object requires a great deal of trust in order for it to effectively accommodate the individual. Considering the fact that our trust is put in a smart object that is of such potential prominence in arguably the ultimate private space, concerns arise regarding the power such a smart object has. It is capable of directing our decisions, opinions and behaviour without most of us being able to identify its "push". Moreover, its power only increases when more smart objects make it into the home that are 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. 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 is compromising not only 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

---

[81] *Supra* n. 77; Eneco Customer Service, personal communication, 19 August 2016.

legislation unless it entails personal data. In the Netherlands, there is a strong push to have a smart thermostat in every home.[82] Combined with the number of other smart objects increasingly entering our house, individuals will not be able to hide much anymore from the state, the entities at the other end of the processes, other individuals with "Toon" in their home, and finally, other residents. Even without specifics such as name or address, this means that the walls are becoming very transparent. It is hard to believe this will not affect the overall feeling of privacy inside the home, and thereby the behaviour of individuals inside their home. Both data protection and the Dutch "home right" fail in this regard to offer meaningful protection of the enjoyment of the individual's private life inside his or her home.

It is true that 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 a single act alone may not say much about an individual, the compilation of everything that goes on inside a home certainly can. As argued before, there is a reasonable expectation of privacy inside the home, even if the services of third parties are used. While reservations should be maintained about the degree and relevant conditions in this context,[83] the mere use of the services of a third party in this way in itself should not. As aforementioned, the smart thermostat cannot be treated the same way as its "dumb" predecessor; it is not just a new or updated version of what once was. The smart thermostat is one of the technological developments capable of bringing on significant changes in society in both behaviour and

---

82 *Supra* n. 41.

83 *Supra* n. 19, p. 171; Mik, "The Erosion of Autonomy" (2016) *supra* n. 21, pp. 28, 39.

communication.[84] 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.

5.2 Smart toys: Hello Barbie

5.2.1 Functions and privacy settings

Where the smart thermostat presents maybe a slight update of the "dumb" thermostat and does not seem to breach any privacy-or data protection laws directly, it does show that profiling and sharing of recorded log-files or other types of metadata generated by devices can lead to behavioural analysis that in turn make for potential breaches of privacy. Taking the harm of behavioural analysis one step further, another set of objects in the home that are turning smart, are toys. Especially when such toys have anthropomorphic features, such as dolls, novel privacy harms might occur as a result.

According to Mattel's fact sheet, "Hello Barbie" is a fashion doll meant as an interactive toy for children from the age of six (according to the manufacturer's recommendation). [85] Children are able to have two-way conversations with this doll, and can play interactive games, since the doll features speech recognition and is able to "learn" from play history to tailor conversations, but it does require a WiFi connection to do so.[86] 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. Parents can monitor, and save or delete the play-history of the

---

84 *Supra* n. 19, p. 185.

85 "Hello Barbie Messaging/Q&A" (2015) available at http://hellobarbiefaq.mattel.com/wp-content/uploads/2015/12/hellobarbie-faq-v3.pdf (accessed 19 July 2017), p. 1.

86 *Ibid.*; Taylor and Michael, "Smart Toys", *supra* n. 1; Manta and Olson, "Hello Barbie", *supra* n. 21, pp. 136-137.

doll with their child via an app that needs to be downloaded first onto a compatible smart object.[87] The frequently asked questions further explains that "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. The doll cannot search the Internet or connect with other toys (for now), but it can connect to the secure servers of ToyTalk (responsible for the speech recognition technology) in the cloud to access dialogue lines.[88] 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, or so advertised. Mattel has indicated that these questions will not entail anything inappropriate (e.g. she will not ask for or respond to the child's name and is programmed as to prevent any swearing) nor are they meant to obtain personal information. While this sounds reassuring, one reporter who was testing "Hello Barbie", 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.[89]

The doll is thus found to make the child divulge its thoughts and opinions.

5.2.2 Privacy and data protection

It is improbable that the child understands that its privacy is violated by its beloved doll, parents, ToyTalk and everyone ToyTalk provides with access, and thus has little say in his or her privacy with regard to the usage of the smart toy.[90] As aforementioned, privacy of the home is an overarching spatial privacy that

---

87 *Supra* n. 85, p. 2.
88 *Ibid.,* pp. 2-3.
89 Taylor and Michael, "Smart Toys" *supra* n. 1, p. 8;
90 *Ibid*., pp. 8-10.

comprises many other objects or privacy depending on the circumstances. In the case of "Hello Barbie", this means that not only privacy of the home is affected, but also of thought, of opinion, and (privacy of) autonomy. In addition, if the findings of the reporter are true, there could be a problem with regard to the mental, economic, cultural or social data collected on the child, by which they might be identified. 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.[91]

The problem for the privacy of the child in this case is that data protection does not extend to the object of protection under, for example, privacy of thought or of the home. 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 other objects of privacy 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 other objects of privacy are compromised. The consequences of this practice in the future for the autonomy of the child and its trust in his or her environment are not yet known since "Hello Barbie" has been brought onto the market very recently.

In terms of potential privacy intrusions, there is another level of threat. 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.

---

91 "Hell No Barbie: 8 Reasons to Leave Hello Barbie on the Shelf" (Campaign for a Commercial-Free Childhood, 1 December 2015) available at http://www.commercialfreechildhood.org/action/hell-no-barbie-8-reasons-leave-hello-barbie-shelf (accessed 19 July 2017).

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 bedroom 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.

Both the smart thermostat and "Hello Barbie" clearly illustrate that concerns and arguments presented in the third and fourth section are not merely theoretical. As argued in the third section, Dutch privacy protection of the home is starting to show significant holes. Moreover, the differences between privacy and data protection as set out in the fourth section are important in practice as well. Although legally some safeguards are in place, there is a mismatch between data protection, which is mainly aimed at protection of personal data, and protection of the home, of which the objective is to manage boundaries of physical entry into the home. Smart devices operate on the boundary of these two, rendering the need for potential novel forms of privacy protection.

6 Conclusion

We argued in this paper that our increasingly smarter homes are seriously affecting the effectiveness of the protection of privacy of the home under the present Dutch legal framework. As already implied in the introduction, the limited definitions of the home and entering actually increase the erosion of the privacy of the home, as both the existing law and application of privacy of the home in the Netherlands are lagging when compared to the rapid advancing development of the Internet of Things and the digitisation of the home. The walls no longer shield the individual effectively from the outside in the pursuing of his

or her personal life without intrusion from the industry and the state.[92] In addition, the absence of *inter alia* a stronger horizontal effect of the "home right" as for Article 8 of the ECHR,[93] and lack of set digital boundaries to the perimeters of the protected home only add to the problem,[94] even more so when considering the tensions between the state and private industry. Data protection is a very important development for privacy, but it cannot substitute privacy, nor can it make up adequately for the erosion of privacy of the home.

The questions raised throughout this paper are likely to only be a small portion of the potential issues that require addressing before the development of the Internet of Things has advanced to the extent that it effectively prevents any reshaping of the legal framework for privacy protection. In order for privacy of the home to remain an effective type of privacy protection for the individual under Dutch law, the time has come to start with revaluating the vision for privacy in the future, and to revisit the existing definitions.

---

92 Koops, van Schooten and Prinsen, "Recht naar Binnen Kijken", *supra* n. 3, pp. 27-28.

93 Kokott and Sobotta, "The Distinction between Privacy and Data Protection" (2013) *supra* n. 66, pp. 225-226; *Supra* n. 28, p.12.

94 Koops and Prinsen, "Glazen Woning", *supra* n. 6, pp. 626-627.

Acknowledgments

Research for this paper was made possible by a grant from the Netherlands Organisation for Scientific Research (NWO), project number 453-14-004. We thank the anonymous reviewers for their helpful suggestions.