Transparency and Consent in Data-Driven Smart Environments

Christof Koolen*

More and more smart devices are making their way into consumers' private homes. While offering convenience, cost and time savings, these internet-enabled objects also raise notable concerns for consumers from a privacy and data protection perspective. Faced with these issues, this paper sheds light on how the principles of transparency and (informed) consent, as well as a recourse to technology, can contribute to a higher level of informational protection for consumers in data-driven smart environments.

Keywords: Transparency | Smart Environments | Data Protection | Internet of Things | Big Data Analytics | Consent

Introduction

The Internet of Things (IoT) has come to be an umbrella term for internet-connected devices with sensory capabilities. These IoT appliances – often referred to as smart devices – take an increasingly prominent role in consumers' daily lives. Connected security systems, remotely controllable lighting, smart wearables, thermostats, refrigerators and even voice-controlled assistants: together, they form an invisible network of information aggregators, capable of capturing data from the physical world and communicating this information via the internet. On the one hand, smart devices undeniably offer practical advantages and useful insights to their users. On the other hand, they also provide the means to compose a detailed account of consumers' behavioral patterns. Combined with big data analytics, it becomes possible to not only anticipate consumers' purchasing preferences, but also to deduce information about their private lifestyles and even map out certain personality traits.

The pervasiveness of smart devices poses challenges that are particularly worrisome from a privacy and data protection perspective. Faced with consumers' concerns regarding the protection and sharing of their personal data, this paper sheds light on the preservation of privacy in smart environments and, more specifically, on the role played by transparency and consent. In this respect, notable emphasis is on (i) awareness surrounding data collection practices and (ii) the implementation of consent mechanisms.

This article features a two-step approach in view of balancing entrepreneurs' thirst for data against consumers' desire for privacy. Firstly, it is necessary to arrive at a solid understanding of the functioning of smart devices in order to better appreciate how the selected transparency concerns manifest themselves in an IoT context (Section I). Secondly, this article takes a closer look at the anatomy and application of transparency (Section II) and consent (Section III) in smart environments. Along this route, attention is given to the notion of 'effective transparency' and the occurrence of 'low-quality consent' among consumers. On balance, this article argues that – notwithstanding transparency and consent – the integration of privacy-enhancing technologies such as obfuscation and data minimization is neces-

DOI: 10.21552/edpl/2021/2/7

* Christof Koolen works as a Ph.D. Researcher at the Institute for Consumer, Competition & Market (KU Leuven, Belgium). He holds a research fellowship from the Research Foundation Flanders (FWO). This paper consists of an adapted version of the presentation done at the Symposium Consumer and Data Privacy: The Digital Revolution of Legal, Social and Economic Interaction, which took place on 24 January 2020 at the Maastricht University, organized by Marta Santos Silva, Kody Moodley, Lisette Bongers, Megan Lana, and Brice Gower and was funded by the University Fund Limburg (SWOL), the Maastricht University Faculty of Law and the Maastricht Working on Europe Research Agenda. The author wishes to express his gratitude to Megan Lana for providing insightful comments and valuable suggestions on the draft version of this paper. For correspondence: <christof.koolen@kuleuven.be>.

sary in view of containing the potential ramifications of data leakages *ex ante* (Section V). In that respect, the question arises to what extent technical rather than legal solutions are necessary in view of attaining adequate levels of privacy and data protection. In conclusion, this article submits that smart environments are putting a strain on the existing regulatory framework, despite potential solutions to transparency and consent more likely stemming from technological and industry-driven efforts (Section VI).

I. Smart Technology, Big Data and the Law

1. All Things Connected

Smart devices are becoming increasingly mainstream nowadays.[1] Due to their convenience factor and affordability, more and more of these smart objects are making their way into consumers' private sphere. Popular devices include smart wearables, which can track users' heart rate, sleep patterns, stress levels, and issue lifestyle recommendations to its wearer based on collected data.[2] In the automotive industry, car sensors can assist drivers, assess the chauffeur's behavior, provide extensive maintenance reports, and even schedule repairs at the local dealership.[3] At home, smart refrigerators[4] are able to tell when the milk has gone stale, and automatically reorder food when required, while smart televisions[5] analyze your viewing habits, and compile personalized suggestions for future viewing. These examples, being just a few in a much longer and rapidly expanding list, give a small insight into the extent to which smart devices have been woven into everyday life.

Alongside the benefits for consumers, smart technology brings with it a new avenue of economic potential, with entrepreneurs actively exploring how to make use of the information gathered by smart appliances to turn a profit.[6] At the core of this trend is the data-driven nature of smart environments, which has significant potential to govern companies' future commercial strategies. The advertising industry, for instance, can rely on the newfound knowledge obtained through means of smart devices to steer particular households towards new commercial products by means of microtargeting.[7] Moreover, given that smart environments provide companies with a steady stream of accurate and real-time information, smart technology also sets the scene for service-dominated business models in many sectors.[8]

The advantages associated with smart technology have sparked the interest of legislators and policymakers as well. The EU, for instance, has recently allocated €500 million to research and testing in the realm of the IoT.[9] Studies indeed highlight that government agencies can benefit from IoT enabled environments as well, with smart technology finding potential application in sectors such as public transportation, healthcare, and public safety.[10] At the same time, however, regulators remain wary of the very intrusive capabilities of IoT ecosystems.[11]

1 IHS Markit, 'Embracing the Internet of Things' (*IHS Markit*, 1 November 2016) <https://cdn.ihs.com/www/pdf/IHS-Embracing-the-IoT.pdf> accessed 7 January 2020; Statista, 'IoT: Number of Connected Devices Worldwide 2012-2025' (*Statista*, 14 November 2019) <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/> accessed 7 January 2020.

2 Samuel Greengard, *The Internet of Things* (MIT Press 2015) 39–40.

3 Lothar Determann and Bruce Perens, 'Open Cars' (2017) 32 Berkeley Technology Law Journal 915, 918–919 and 945–946.

4 Aurelia Tamò-Larrieux, 'Privacy Protection in an Internet of Things Environment' in Aurelia Tamò-Larrieux (ed), *Designing for Privacy and its Legal Framework* (Springer International Publishing 2018) 47.

5 Samsung, 'Samsung Privacy Policy for the U.S.' (*Samsung Electronics America*, 1 January 2020) <https://www.samsung.com/us/account/privacy-policy/> accessed 10 January 2020.

6 Natali Helberger, 'Profiling and Targeting Consumers in the Internet of Things – A New Challenge for Consumer Law' (2016) SSRN Scholarly Paper 10 <https://papers.ssrn.com/abstract=2728717> accessed 8 January 2020.

7 Natali Helberger, Frederik Zuiderveen Borgesius and Agustin Reyna, 'The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection' (2017) 54 Common Market Law Review 1427, 1430.

8 Janja Hojnik, 'The Servitization of Industry: EU Law Implications and Challenges' (2016) 53 Common Market Law Review 1575, 1581–1582.

9 European Commission, 'Research & Innovation in Internet of Things' (*Digital Single Market - European Commission*, 28 April 2016) <https://ec.europa.eu/digital-single-market/en/research-innovation-iot> accessed 14 January 2020.

10 OECD, 'The Internet of Things: Seizing the Benefits and Addressing the Challenges' (2016) 17 <https://www.oecd-ilibrary.org/science-and-technology/the-internet-of-things_5jlwvzz8td0n-en> accessed 19 November 2019; Stefania Aguzzi and others, 'Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination: Final Report' (European Commission Publications Office 2014) 49.

11 Inge Graef, Damian Clifford and Peggy Valcke, 'Fairness and Enforcement: Bridging Competition, Data Protection, and Consumer Law' (2018) 8 International Data Privacy Law 200, 211.

2. Implications of Big Data

While the features and benefits of smart objects may explain their rise in popularity, the implications of large-scale data stockpiling also elevate the risk of data misuse. Compiling data from different smart devices leads to the creation of so-called 'big data lakes'[12], which can subsequently be parsed by data science toolkits and machine learning algorithms. By enabling the analysis of information in the context of other information, it becomes possible to uncover patterns and connections, which are not obvious at first sight.[13] On the one hand, this puts companies in a position to better understand and target their customers, for instance by predicting their willingness to pay for a certain product.[14] On the other hand, however, the collection and processing of personal information also comes with inherent risks, which may not always be obvious to the average consumer.[15]

A first concern relates to the fact that undertakings are particularly keen on collecting and processing data that are not strictly necessary for the proper functioning of a smart device. Connected devices often come with onerous privacy statements, which are presented on a 'take it or leave it' basis to consumers, and which offer little to no leeway to limit the scope of data processing activities. This ties into a second concern, namely awareness surrounding data stockpiling. Even though consumers may be willing to share some personal details, it is not unheard of that they are not fully aware of the extent and consequences of companies processing their data.[16] A third issue concerns the heavy reliance on big data analytics. While algorithms are needed to bring order to the chaos of data, there exists an inherent risk of drawing inaccurate conclusions from available datasets (e.g. due to misinterpretation or due to having wrong or incomplete information).[17] This could give rise to situations where, to the detriment of consumers, banks mistakenly reject particular loan applications or insurance companies erroneously deny coverage. A fourth problem involves businesses that rely on big data in an attempt to exercise *undue influence*[18] over consumers' decision-making processes (e.g. the exploitation of personal biases) or to engage in discriminatory or exclusionary marketing.[19] By way of illustration, one could think of aggressively advertising weight loss supplements to consumers who recently used Google search parameters such as 'how to lose weight'. A fifth matter revolves around companies invariably being in a position to misuse or misappropriate collected personal information, for instance by disclosing or transferring data to third parties without consumers' prior consent.[20] A sixth and final aspect relates to data security.[21] The inherent result of large-scale data stockpiling is the creation of so-called honey pots filled with up-to-date information on thousands of people. These honey pots form a prime target for hacking attempts – as illustrated by a number of high-profile data breaches during the last few years. The underlying issue is that consumers often have no way of ascertaining whether companies are taking adequate safeguards to store their personal information. This proves problematic, especially in the knowledge that, presently, potential data breaches lurk around every corner.

It should come as no surprise that entrepreneurs have a strong appetite for processed data in the sense that it grants them a better understanding of their target market and enables them to create '*value from connections*'[22]. In that way, data has slowly evolved

12 Swaroop Poudel, 'Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security Cyberlaw and Venture Law' (2016) 31 Berkeley Technology Law Journal 997, 1006.

13 ibid.

14 Wolfgang Kerber, 'Digital Markets, Data, and Privacy: Competition Law, Consumer Law and Data Protection' (2016) 11 Journal of Intellectual Property Law & Practice 856, 858.

15 Stacy-Ann Elvy, 'Commodifying Consumer Data in the Era of the Internet of Things' (2018) 59 Boston College Law Review 423, 448–449.

16 Viktoria Robertson, 'Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data' (2020) 57 Common Market Law Review 161, 183; Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR)* (Springer International Publishing 2017) 241; Article 29 Working Party, 'Opinion 8/2014 on the on Recent Developments on the Internet of Things' (2014) Guideline 14/EN WP 223 3.

17 Helberger, Borgesius and Reyna (n 7) 1435.

18 Article 2(j), Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market [2005] OJ L149/22 defines undue influence as 'exploiting a position of power in relation to the consumer so as to apply pressure, even without using or threatening to use physical force, in a way which significantly limits the consumer's ability to make an informed decision'.

19 Helberger, Borgesius and Reyna (n 7) 1430.

20 Elvy (n 16) 455.

21 Thomas Hoppner and Anastasia Gubanova, 'Regulatory Challenges of the Internet of Things' (2015) 21 Computer and Telecommunications Law Review 227, 229.

22 Laurent Probst and others, 'Smart Living: Connected Devices for Intelligent Homes' (European Commission 2014) <https://ec.europa.eu/docsroom/documents/13407/attachments/5/translations/en/renditions/pdf> accessed 12 June 2020.

into a new commodity and a means to monetize consumers' individual attention units.[23] However, when it comes to data collection, processing, and usage, it is apparent that a number of notable challenges arise once consumers allow smart objects to enter into their private homes.

3. Legal Framework

Relying on smart technology triggers the following question: how to balance consumers' privacy against smart devices' efficacy?[24] At present, it is often difficult to discern between legitimate and unlawful data collection, given the multitude of considerations that come into play. These considerations include not only the context surrounding data stockpiling and the methods of data collection, but also the applicable legal rules.

At the outset, it is worth noting that privacy and data protection are strongly connected but not the same.[25] Whereas privacy predominantly concerns intrusions into one's private life, data protection revolves around information practices[26] and, more specifically, the permissibility of processing personal information.[27] Legal scholarship indicates, however, that overlaps exist between the right to privacy and the right to data protection, given that data protection issues oftentimes involve privacy issues as well.[28] In that regard, the argument goes that data protection could – at least to some extent – be subsumed under the concept of privacy.[29]

For all intents and purposes, there do not exist industry-specific privacy and data protection rules to regulate the Internet of Things. However, both the right to privacy and data protection are enshrined in different human rights treaties – such as the CFR[30] and the ECHR[31]. Evidently, these provisions apply to smart environments as well. With the entry into force of the General Data Protection Regulation[32] (GDPR) in 2018, the EU also took a clear stance towards consumer data protection. Moreover, processing activities performed by smart devices can also trigger the application of the ePrivacy Directive[33] (hereafter: ePD), which constitutes a *lex specialis* to the GDPR.[34]

In light of the ability to map out the consumer's behavioral patterns and identify his/her personal preferences, the risk of smart device data being abused or misappropriated (e.g. through means of targeted manipulation or misleading marketing practices) should not be overlooked.[35] Notwithstanding the existence of certain legal rules, it remains a difficult task to apply the often broadly worded provisions to new phenomena such as smart technology. As a result, the IoT and, by extension, data-driven smart environments give rise to new legal complications vis-à-vis privacy and personal data protection.[36]

In the author's view, it is neither feasible nor desirable to impose outright legislative restraints on the development, production, or capabilities of smart devices in order to overcome these challenges. Instead, in the face of data-aggregating smart environments, this article considers how the principles of transparency and (informed) consent can contribute to a higher level of privacy and data protection for consumers. The interplay between these two concepts is central to the establishment of a robust and consumer-centric framework for data processing activities: undertakings must first provide meaningful information about how they wish to collect and use consumers' personal data before those consumers can validly consent to data processing.

---

23 See for instance Elvy (n 15).

24 Jillisa Bronfman, 'Weathering the Nest: Privacy Implications of Home Monitoring for the Aging American Population' 14 Duke Law & Technology Review 192, 199.

25 Tamò-Larrieux (n 4) 73; Raphaël Gellert and Serge Gutwirth, 'The Legal Construction of Privacy and Data Protection' (2013) 29 Computer Law & Security Review 522, 526; Juliane Kokott and Christoph Sobotta, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3 International Data Privacy Law 222, 223.

26 Gellert and Gutwirth (n 25) 525.

27 Tamò-Larrieux (n 4) 74.

28 Kokott and Sobotta (n 25) 227–228.

29 Gellert and Gutwirth (n 25) 526.

30 Charter of Fundamental Rights of the European Union.

31 European Convention on Human Rights.

32 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1.

33 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37.

34 European Data Protection Board, 'Opinion on the interplay between the ePrivacy Directive and the GDPR' (2019) Opinion 5/2019 12.

35 Rolf Weber, 'Internet of Things: Privacy Issues Revisited' (2015) 31 Computer Law & Security Review 618, 619.

36 ibid; Tamò-Larrieux (n 4) 51; Gilad Rosner and Erin Kenneally, 'Privacy and the Internet of Things - Emerging Frameworks for Policy and Design' (2018) CLTC Occasional White Paper Series 6.

II. Transparency

1. Substance of the Transparency Requirement

At its core, transparency involves an element of 'making someone aware of something'. The general idea behind the principle of transparency is to level the playing field and remedy information asymmetries, which often exist between consumers and (more knowledgeable) traders. Therefore, transparency obligations enhance consumers' position by providing them with information that subsequently enables them to make well-informed transactional decisions.[37]

In the context of smart technology and data protection, however, it is presently more accurate to speak of translucency rather than transparency. Although consumers might have a general idea of what happens with their personal information, ongoing technological developments often make it difficult to fully grasp the privacy implications of data processing.[38]

A closer look at some of the relevant EU rules in this area provides more clarity regarding the substance of the transparency requirement. The Consumer Rights Directive[39] (hereafter: CRD), for instance, contains various information disclosure duties, according to which traders must produce clear and comprehensive information to consumers regarding the main characteristics of any goods or services that are the subject of a business-to-consumer agreement. Transparency obligations also extend to contractual clauses. According to the Unfair Contract Terms Directive[40] (hereafter: UCTD), contract terms must be drafted in plain and intelligible language.[41] In essence, this requirement consists of two separate components.[42] From a formalistic angle, this implies that consumers should be able to easily access and become acquainted with the terms and conditions of an agreement. From a substantive point of view, the information supplied by the trader also needs to be understandable to the average consumer. More recently, the principle of transparency is also relied on as a tool intended to improve consumers' understanding vis-à-vis the processing of their personal data.[43] In that respect, the GDPR comes into view.[44] What is interesting is that the GDPR differs from the CRD and the UCTD: whereas the latter two instruments predominantly deal with contractual situations, the former specifically relies on data as the operative word. Accordingly, the GDPR mandates that data controllers should provide data subjects with information regarding the collection, use or processing of their personal data. This information should be made available in clear and plain language as well as being '*easily accessible and easy to understand*'.[45] As a *lex specialis* to the GDPR, article 5(3) ePD adds an important additional proviso.[46] Since consumers' internet-connected smart devices qualify as "terminal equipment"[47] under the Directive, undertakings must also disclose in a clear and comprehensible manner when and for what purposes they wish to store information in or access data from these devices.[48]

Within the existing consumer law framework, the implications of digital technology often remain un-

37 Geraint Howells, Christian Twigg-Flesner and Thomas Wilhelmsson, *Rethinking EU Consumer Law* (Routledge 2018) 95.

38 The GDPR defines processing in art 4(2) as: '*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*'; Ugo Pagallo, Massimo Durante and Shara Monteleone, 'What Is New with the Internet of Things in Privacy and Data Protection? Four Legal Challenges on Sharing and Control in IoT' in Ronald Leenes and others (eds), *Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer International Publishing 2017) 63.

39 Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights [2011] OJ L304/64.

40 Council Directive 93/ 13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L95/29.

41 Evelyne Terryn, 'Transparantie En Algemene Voorwaarden - Nood Aan Hervorming?' [2017] Tijdschrift voor Privaatrecht 13, 19.

42 Marco Loos, 'Transparency of Standard Terms under the Unfair Contract Terms Directive and the Proposal for a Common European Sales Law' (2015) 23 European Review of Private Law 179, 180.

43 Weber (n 35) 625.

44 Art 5(1)(a), GDPR; art 12, GDPR.

45 Recital 39, GDPR.

46 Art 5(3), ePD is a general provision and, therefore, does not exclusively apply to electronic communication services. As a result, data processing activities via internet-connected smart devices also fall under its scope.

47 Art 1(1), Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment [2008] OJ L162/20: '"terminal equipment" means: equipment directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information'.

48 European Data Protection Board, 'Guidelines on Processing Personal Data in the Context of Connected Vehicles and Mobility Related Applications' (2020) Guideline 1/2020 5–6.

derexposed. The entry into force of the Omnibus Directive[49] attempts to address some of these concerns by updating numerous existing consumer protection rules in light of the '*continuous development of digital tools*'.[50] Faced with new, digital means to facilitate marketing practices – such as automated decision-making and personalized pricing – traders are now under an obligation to inform consumers when they rely on such tools.[51] Moreover, multiple authors argue that the fairness rationale behind the UCTD could find application to privacy contracts as well.[52] In that sense, clauses in privacy policies can be regarded as unfair if, contrary to the requirement of good faith, they create a significant imbalance between the position of the data subject and data controller.[53]

In the current state of affairs, one could argue that consumer law and data protection law can be perceived as being reciprocal and mutually advantageous to one another, especially in a digital context. While this strand of reasoning has not been fully developed yet, there are some distinct advantages associated with doing so. For instance, consumer law could act as a secondary line of defense to curb data processing behavior that may well be acceptable under the GDPR, but not necessarily under consumer law. Moreover, the interplay between consumer law and data protection law also creates a possibility to rely on the technical jargon from data protection law (e.g. data minimization, privacy by default) while interpreting the fairness criterion from consumer law.[54] Furthermore, data subjects could invoke the fairness and transparency argument as a means to force undertakings to comply with the substantive principles contained in data protection law. As the law currently stands, however, many of these aspects remain unclear and the current legal framework does not adequately address existing problems relating to smart technology.

2. Applying the Transparency Criterion to Smart Environments

Two elements follow from the previous section. Firstly, it is apparent that several legal instruments exist that effectuate more transparency for consumers on the market. Secondly, despite the existence of these instruments, it presently remains difficult to apply the principle of transparency to smart environments due to the inherent complexity and rather technical nature of smart devices. This unspoken tension between theory and practice calls for action: the principle of transparency needs to find application in a functional way in smart environments. In light of this, this section aims to clarify and give substance to the notion of transparency, specifically when applied to smart devices. Given the novelty and evolving nature of this topic, however, it is difficult to assert claims *de lege lata* as to how exactly transparency applies in smart environments. Instead, the goal of this section is to illustrate how one *could* interpret and apply the existing legal provisions in the face of a new technological phenomenon.

In the author's view – and within the scope of this article – the principle of transparency has a twofold dimension when applied to an IoT context: a consumer angle and a business angle. On the one hand, consumers should be able to identify which smart devices are present in their direct surroundings and understand which particular bits of data smart devices are capturing. Legally speaking – and perhaps surprisingly – the transparency requirement contained in article 5(1)(a) and article 13 of the GDPR does not mandate the disclosure of the specific categories of collected personal data if these data have been directly obtained from the data subject.[55] However, interpreting and applying these provisions as such would arguably go against the underlying rationale

49 Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules [2019] OJ L328/7.

50 Recital 17, CMD.

51 Recital 45, CMD and art 4(4)(a)(ii), CMD; Tycho de Graaf, 'Consequences of Nullifying an Agreement on Account of Personalised Pricing' (2019) 8 Journal of European Consumer and Market Law 184, 185.

52 Michiel Rhoen, 'Beyond Consent: Improving Data Protection through Consumer Protection Law' (2016) 5 Internet Policy Review 1, 7; Helberger, Borgesius and Reyna (n 7) 1451; Peter Rott, 'Data Protection Law as Consumer Law - How Consumer Organisations Can Contribute to the Enforcement of Data Protection Law' (2017) 6 Journal of European Consumer and Market Law 113, 114–115.

53 cf. Council Directive 93/ 13/EEC of 5 April 1993 on unfair terms in consumer contracts (n 40), art 3.

54 Helberger, Borgesius and Reyna (n 7) 1451.

55 Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (2018) Guideline 17/EN WP260 rev.01 36; note that, pursuant to article 14(1)(d) GDPR, the disclose of the categories of collected personal data is required if the data is not obtained from the data subject.

of providing a high level of protection for natural persons.[56] When testing this line of reasoning against the benchmark of the average, reasonably well-informed consumer, it is fair to state that information pertaining to the data collection aspects of smart devices can sway the decision-making process of end users. On the other hand, businesses should also clearly and fully inform consumers regarding their intentions once the data have been collected. Therefore, in order to facilitate better-informed decisions when purchasing smart devices, a combined reading of the transparency requirements contained in articles 5-6 CRD and articles 5-6 GDPR should also take some additional considerations into account regarding high-tech appliances.[57]

Firstly, consumers should receive more details regarding the *functionality* of smart appliances before committing to a purchase (cf. article 6(1)(r) CRD). In that regard, alongside mentioning a smart device's essential product characteristics, the mandatory pre-contractual information obligations could perhaps also shed light on the types of sensors, which are embedded in the particular device, as well as their data capturing abilities.[58] If, for instance, a smart TV has the ability to be turned on via voice commands, it is perhaps useful to make users aware of the TV's passive listening abilities. Other elements that come to mind are the effective sensor range and the data capture frequency.

Secondly, the smart appliance itself should properly indicate what *categories of (personal) information* it captures (cf. article 5(1)(a) GDPR).[59] While it is obvious that certain types of smart devices possess the ability to capture certain types of information, it is not always clear how far this goes. For instance, consumers may find it plausible that a smart thermostat captures information on direct temperature adjustments and energy consumption trends. However, they might not necessarily be aware that the device also collects information entered during the set-up procedure as well as environmental and ambient data.[60] A new, modern take on interpreting the transparency requirements should alleviate these information asymmetries.[61] In doing so, consumers themselves can also more easily deduce which information businesses could potentially infer from collected data.

Thirdly, smart device retailers should be transparent about their motivations as to why certain data needs to be captured, for what purposes it is processed and with whom it is shared (cf. article 5(1)(b) GDPR and article 5(3) ePD). In that respect, any *statement of purpose* needs to be clear and precise.[62] In contrast, vaguely worded catch-all statements do not meet this threshold.[63] Consider, for instance, the following example from a privacy policy: '*We may use the information we obtain to [...] improve our services*'.[64] In the eyes of the author, this phrase provides sufficient coverage to explain why a smart device collects usage analytics about itself and transmits them back to the retailer. However, this statement is not sufficiently precise to explain why geolocation data of the user needs to be captured as well. A better-suited reason would be to mention that the collection of geolocation data facilitates the prevention of identity theft or unauthorized account access.[65] In line with this reasoning, collecting data for interest-based advertising purposes is not in itself problematic as long as the aggregating entity clearly and precisely communicates these intentions to the consumer in accordance with the GDPR, the ePD, and overarching transparency rules under EU consumer law. Regrettably, this is not always the case in practice.

3. Consumer Apathy, Attrition and Disinterest

The three elements from the previous section give substance to the overall transparency requirement.

56 Recitals 6 and 10, GDPR.

57 The views set out in Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (2018) Guideline 17/EN WP260 rev.01 are instrumental to this analysis.

58 Victor Morel and others, 'Enhancing Transparency and Consent in the IoT', *IWPE 2018 - International Workshop on Privacy Engineering* (2018) 118 <https://hal.archives-ouvertes.fr/hal-01709255 > accessed 17 January 2020.

59 Robert Szewczyk, 'Transparency in IoT' (2015) Stanford Secure Internet of Things Project <http://iot.stanford.edu/retreat15/sitp15 -transparency-no.pdf> accessed 18 January 2020.

60 ibid.

61 Article 29 Working Party, 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (n 16), 6.

62 Note that the GDPR refers to the principle of purpose limitation on multiple occasions. In that regard, see, for instance, art 5(1)(b), GDPR and art 6(1)(a), GDPR.

63 Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (n 55), 9.

64 Samsung (n 5).

65 ibid.

Yet, there are a number of limitations and drawbacks associated with merely providing consumers with more information regarding their products. Consumer apathy is one of them.[66] With privacy policies often being in excess of 5000 words, many consumers – even those concerned about their privacy – simply cannot be bothered to read all documents in their entirety. Due to this, the pre-contractual information obligations may attain exactly the opposite of what they are meant to achieve, namely better informing consumers.

It is worth pointing out that some studies are already underway to identify and solve issues relating to rational apathy.[67] Intermediary research results indicate that a number of recurring problems exist in privacy policies, which have significant potential to trigger consumer attrition. These problems often relate to the illegibility, complexity, and vagueness of standard Terms & Conditions as well as their excessive length and incomparability with other texts.[68] A number of solutions are put forward as well, such as providing short summaries of the Terms & Conditions, layered privacy notices, FAQs, icons, reading time estimations or even introducing an element of gamification.[69] Avenues explored by other researchers include parsing Terms & Conditions through means of artificial intelligence in order to verify whether certain clauses comply with the GDPR.[70] In light of these initiatives, it is both necessary and useful to reflect on the current form and manner in which pre-contractual information is presented to consumers. If anything, steps should be taken towards making existing privacy policies less text-heavy[71] and more visually appealing.

Apart from rational apathy, the limitations of the medium should also be taken into account. Presenting a lengthy privacy policy is simply not viable via a 16 cm² smart watch display and near impossible for a screenless smart speaker. The CRD considers this specific limitation in article 8(4) and sets out that consideration needs to be given to the particular medium. In terms of a potential workaround, it is worth reflecting about making use of gateway devices – for example a smartphone or a pc – in order to convey all the necessary details.

Lastly, one strand of argument also emphasizes that some consumers do not particularly mind that undertakings collect and process their personal information. This lackadaisical attitude towards privacy finds its basis in various reasons and explanations.[72] For instance, some consumers might prefer to be early adopters of new technology, thereby showing a strong indifference towards their privacy.[73] Others might take a more relaxed approach to data protection simply because '*they prefer cheaper or trendier products*'.[74] Another reason, which often surfaces, is the '*I've got nothing to hide*'-argument.[75] Academics in the US also found that consumers often hold a sentiment of '*whatever*' towards privacy due to quality (e.g. reading difficulties) and quantity (e.g. accumulation of privacy policies, information overload) problems associated with information disclosures.[76] In terms of functionality, some consumers also prefer to make use of their internet-connected appli-

66 Lillian Ablon and others, *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information* (RAND Corporation 2016) 26–28.

67 Arianna Rossi and others, 'When Design Met Law: Design Patterns for Information Transparency' (2019) 122–123 Droit de la consommation - Consumentenrecht 79; Rossana Ducato and Alain Strowel, 'Information Duties between Consumer and Data Protection in the "Internet of Platforms": Promoting Awareness by Design' (2019) 122–123 Droit de la consommation - Consumentenrecht 123.

68 Rossi and others (n 67) 91–98.

69 ibid 98–120.

70 X, 'Claudette - Machine Learning Powered Analysis of Consumer Contracts and Privacy Policies' (*Claudette*) <https://claudette.eui.eu/> accessed 2 March 2020; Giuseppe Contissa and others, 'Claudette Meets GDPR: Automating the Evaluation of Privacy Policies Using Artificial Intelligence' (2018) SSRN Scholarly Paper <https://www.ssrn.com/abstract=3208596> accessed 2 March 2020.

71 Stefania Passera, 'Beyond the Wall of Text: How Information Design Can Make Contracts User-Friendly' in Marcus Aaron (ed), *Design, User Experience, and Usability: Users and Interactions* (2015) 341–352.

72 For a deeper discussion and typology of the different attitudes towards privacy, see: Isioma Elueze and Anabel Quan-Haase, 'Privacy Attitudes and Concerns in the Digital Lives of Older Adults: Westin's Privacy Attitude Typology Revisited' (2018) 62 American Behavioral Scientist 1372-1391.

73 See, for instance, Cynthia Cheung and others, 'Privacy Attitudes among Early Adopters of Emerging Health Technologies' (2016) 11 PLoS ONE 5: 'Our sample of early adopters expressed more "pragmatic" and "unconcerned" type privacy beliefs [...] than would be expected from the general public. In spite of this, it is notable that participants were both highly aware of and actively considering "fundamentalist" privacy concerns'.

74 Bronfman (n 24) 221.

75 Daniel Solove, '"I've Got Nothing to Hide" and Other Misunderstandings of Privacy' (2007) 44 San Diego Law Review 745, 748.

76 Omri Ben-Shahar and Carl Schneider, *More Than You Wanted To Know: The Failure of Mandated Disclosure* (Princeton University Press 2014) 59 et seq.

Figure 1 - Illustration of what a privacy push notification could look like.

ances to their fullest extent, regardless of the (data) cost. This implies, for instance, that receiving interest-based advertisements based on personal data is sometimes seen as a positive feature rather than a shortcoming.

4. Towards Effective Transparency

Taken altogether, these concerns highlight that different interests are at stake and, moreover, they put question marks over the current application of the transparency principle. In light of consumers being mostly rationally apathetic and the phenomenon of consumer attrition, it is presently not tenable to rely on the assumption that all consumers are 'deemed to have read' privacy policies. For those reasons, the author of this article advocates for *effective transparency* rather than *full transparency*. Transparency should be effective in a sense that it is able to achieve what it is meant achieve, namely better informing consumers. The challenges posed by smart environments and the IoT, therefore, call for a fitting application of the transparency principle. This implies that neither an information overload (e.g. misguided attempts to provide consumers with extensive and detailed technical information) nor completely slimmed down information disclosures (e.g. bullet point summaries) are desirable.

a. Push Notifications

In search of a middle-ground solution, scholars have suggested elsewhere that the use of notifications might be well suited for this purpose.[77] For instance, if a consumer recently bought a new smart wearable and he relies on this device to keep track of his daily physical activities, he might receive a push notification on the device during the evening that mentions: '*Your data is about to be synchronized with our cloud servers. Click here to disable this feature.*' Similarly, if a consumer issued a voice command to his smart speaker, a notification could show up on his phone immediately afterwards, reminding the user of the voice analysis process that takes place in the background. Smart appliances could also consider users' previous privacy preferences. Consider, for example, the following notice: '*You chose not to store GPS data when you are outside a one-mile radius of your home; would you also like to disable automatic check-ins at fitness facilities?*'[78] One of the advantages of using notifications is that they are able to get the message across in a short and concise manner without being particularly intrusive. Moreover, smart device manufacturers can easily tailor notification procedures to suit the consumer's wishes: providing context-specific notifications, periodic reminders or layered notifications are all possible.[79] If the consumer so desires, he could even disable the notification system altogether after a while. Although there exists no empirical evidence that corroborates the efficiency of such push notifications at present, the author does see merit in these small nudges as they *prima facie* seem to have fair potential to enhance transparency for consumers.

However, the recommendation outlined in the previous paragraph also triggers wider regulatory complications. More specifically, it can be questioned how increasingly technical suggestions for improvement can be transposed into legally enforceable requirements for smart device manufacturers. Against this backdrop, it should be noted that any attempt to transpose technical transparency mechanisms into law might also bring about a risk of stifling innova-

77 Rosner and Kenneally (n 36) 16.

78 ibid 18.

79 ibid 16–17.

tion.[80] As a result, a one-size-fits-all approach to enhancing transparency is, in all likelihood, neither feasible nor desirable due to the large variety and complexity that exists among smart devices.

b. Competing for Transparency

Conversely, maintaining the status quo position does not seem preferable either. Instead, in view of stimulating further discussion on this topic, it might be worth considering introducing an element of competition between producers of smart devices. For instance, a privacy grading or scoring system based on a smart device's level of intrusiveness could prove useful to quickly inform consumers about any associated privacy implications. In that regard, inspiration could be drawn from the current EU energy labeling scheme[81] (i.e. a ranking based on letters that are linked to a color scheme ranging from green to red). Smart devices that come with particularly onerous or unintelligible privacy policies would receive a lower score compared to their more privacy-friendly counterparts. Ideally, smart device manufacturers, fueled by a desire to generate more sales revenue, would perceive this as an impetus to offer a higher level of data privacy to consumers. Although this idea comes with its own share of challenges, recent developments such as the previously mentioned AI-based parsing tool for Terms & Conditions could provide the necessary foundation to turn this idea into reality. A close study of Apple's "privacy nutrition labels", introduced in December 2020 for applications in the Apple App Store, may also prove useful.[82] In any event, it becomes apparent that smart environments often fall short of providing an appropriate level of transparency to consumers. Moreover, at present, there seems to be no clear answer to the question as to how exactly to enhance transparency given the rapidly evolving nature of smart technology.

III. Consent

1. Substance of the Consent Requirement

As mentioned earlier,[83] the GDPR and ePD impose extensive information disclosure requirements on entities that engage in the processing of personal data.[84] The goal of such stringent rules is to create an environment of transparency and clarity for consumers. However, transparency in itself does not suffice: lawful data processing can only take place if the data controller or processer is able to rely on selected grounds that justify processing (article 6 GDPR).[85] This implies, for instance, that data aggregating entities are entitled to process information if this is necessary for the performance of a contract[86] or needed in order to comply with a legal obligation[87]. The pursuit of legitimate interests[88] is also listed among the lawful processing grounds.

In the context of consumer data privacy, however, the aforementioned rules put a notably strong emphasis on consent as a legitimate ground for data processing.[89] This is not only the case under the GDPR, but also pursuant to article 5(3) ePD; a provision which takes precedence over the grounds for lawful data processing contained in article 6 GDPR.[90] According to article 5(3) ePD, data processing operations that specifically involve accessing or storing information in terminal equipment of consumers must rely on prior consent of that consumer.[91] This should come as no surprise: having a full understanding of

80 ibid 14.

81 European Commission, 'Energy Label and Ecodesign' (*European Commission*) <https://ec.europa.eu/info/energy-climate-change-environment/standards-tools-and-labels/products-labelling-rules-and-requirements/energy-label-and-ecodesign_en> accessed 18 March 2020.

82 Apple, 'App Privacy Labels Now Live on the App Store' (*Apple - Developer News and Updates*) <https://developer.apple.com/news/?id=3wann9gh> accessed 18 February 2021; Apple, 'Data Privacy Day at Apple: Improving Transparency and Empowering Users' (*Apple - Newsroom*) <https://www.apple.com/newsroom/2021/01/data-privacy-day-at-apple-improving-transparency-and-empowering-users/> accessed 18 February 2021.

83 See above at II.1.

84 Art 6(1)(a), GDPR; recital 39, GDPR.

85 Voigt and von dem Bussche (n 16) 88.

86 Art 6(1)(b), GDPR.

87 Art 6(1)(c), GDPR.

88 Art 6(1)(f), GDPR.

89 Yves Poullet, 'Consentement et RGPD: Des Zones d'ombre' (2019) 122–123 Droit de la consommation - Consumentenrecht 3, 5.

90 European Data Protection Board (n 48) 5–6.

91 A fitting example of this line of reasoning can be found in a recent ruling handed down by the French Data Protection Authority against Google: Délibération SAN-2020-012 du 7 décembre 2020, *Google LLC et Google Ireland Ltd* [2020] SAN-2020-012; an English press release is available here: Commission Nationale de l'Informatique et des Libertés, 'Cookies: Financial Penalties of 60 Million Euros against the Company Google LLC and of 40 Million Euros against the Company Ireland Limited' (*CNIL*, 10 December 2020) <https://www.cnil.fr/en/cookies-financial-penalties-60-million-euros-against-company-google-llc-and-40-million-euros-google-ireland> accessed 19 February 2021.

any ongoing data processing activities allows for data subjects to cater to their own interests. Thus, consent entails an element of autonomy[92], which is not present in any of the other grounds of lawful data processing. For that reason, consent bears the label of representing the pinnacle of '*informational self-determination*'.[93] Aside from this, it is worth noting that the GDPR substantially strengthens the specific requirements for consent beyond what one would normally expect.

Accordingly, in order to be valid, any data subject's consent to data processing requires compliance with a specific subset of criteria. Pursuant to article 4(11) GDPR, consent needs to be '*freely given, specific, informed and unambiguous*'.[94] Apart from Recital 32 and the fact that consent calls for an element of 'signifying agreement'[95], the GDPR itself does not further expand on these four sub-criteria. The four elements of valid consent were, however, discussed at length by the Article 29 Working Party (Art. 29 WP), an advisory body tasked with providing expert advice on the topic of EU data protection.[96] Their findings were subsequently published in a 31-page guideline.[97]

2. Applying the Consent Requirement to Smart Environments

Each criterion for consent has attracted extensive commentary in legal doctrine.[98] At this point, it is worth assessing how scholars interpret the different criteria for consent and how they find application in smart environments. The views put forward by the Art. 29 WP in their Guidelines on Consent under Regulation 2016/679 will play a significant role in this analysis.

First and foremost, consent needs to be *freely given*. This involves an element of real choice on behalf of the data subject.[99] Moreover, this also denotes that consumers should be able to refuse subjection to data processing or even withdraw their consent without serious detriment.[100] However, practices such as making the performance of a contract or the provision of a service conditional upon consent risk nullifying the given consent altogether.[101] Consider, for instance, a smart wearable, which not only measures wearers' heart rate and steps taken, but which also keeps track of their location. In this situation, the heart rate sensor is fully capable of functioning entirely independent from the GPS. If the wearable makes the functioning of the heart rate monitor conditional on giving consent to the collection of geolocation data (i.e. tying consent), then this can hardly constitute freely given consent. Instead, it would be more accurate to describe these situations as providing transparency without choice. As mentioned in this paragraph, the answer would be different if the bundling of different elements is genuinely necessary for a smart device to function properly. A factual analysis thus seems most appropriate to assess the 'freely given' criterion, especially in light of the rather complex nature of smart appliances.

Consent also needs to be *specific*, as pointed out in article 6(1)(a) GDPR. The prevailing interpretation suggests that specificity relates to two separate elements: (i) the categories of collected personal data and (ii) the purpose of collecting those data. A combined reading of the GDPR and the Art. 29 WP Guidelines also highlights that this criterion implies granularity: the data subject should be able to choose which data processing aspects they would like to accept or refuse.[102] In the author's view, the specificity requirement demonstrates anew the importance of transparency, choice, and user control. For example, if a data controller or processor fails to adequately disclose what information their smart device collects and for what purposes, this could potentially invalidate the data subject's consent. The same line of

92 Eleni Kosta, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers 2013) 133.

93 Poullet (n 89) 5; Kerber (n 14) 857; Kosta (n 92) 133–134.

94 Art 4(11), GDPR; Morel and others (n 58) 117; Georgia Skouma and Laura Léonard, 'On-Line Behavioral Tracking: What May Change After the Legal Reform on Personal Data Protection' in Serge Gutwirth, Ronald Leenes and Paul de Hert (eds), *Reforming European Data Protection Law*, vol 20 (Springer Netherlands 2015) 52.

95 Art 4(11), GDPR.

96 European Data Protection Board, 'Article 29 Working Party' (*European Data Protection Board*, 10 January 2018) <https://edpb.europa.eu/our-work-tools/article-29-working-party_en> accessed 17 January 2020.

97 Article 29 Working Party, 'Guidelines on Consent under Regulation 2016/679' (2018) Guideline 17/EN WP259 rev.01.

98 See, for instance, the seminar work on consent by Eleni Kosta: Kosta (n 92).

99 Article 29 Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 97) 5.

100 Pagallo, Durante and Monteleone (n 38) 64; Poullet (n 89) 6.

101 Article 29 Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 97) 5.

102 ibid 11.

reasoning extends to situations where undertakings require general or catch-all consent rather than offering consumers a possibility to give specific consent to some data processing activities while denying consent to other aspects of data collection.

A third element revolves around consent being *informed*. As with the previous criterion, this calls for the provision of information from the data collecting entity to the data subject.[103] Similar to the pre-contractual information requirements under the CRD, one can expect that it is mandatory to mention the identity, address, and contact information of the data controller. Especially with regard to data collection, data controllers should mention the types of data and the purposes of any processing operations in view of obtaining valid consent. However, merely providing information does not necessarily mean that a data subject is able to understand it. For that matter, the data collecting entity should steer away from using language that is difficult to understand or phrasing that contains overly complex legal jargon. The GDPR does not prescribe the specific instrument or form as to how this information should be delivered to the end user, while the Art. 29 WP hints at the possibility of both written and oral statements as well as audio and video messages.[104]

Lastly, the data subject has to provide an *unambiguous* indication of consent. The GDPR further describes this as '*a statement or a clear affirmative action*'.[105] A close reading of the text suggests that a flexible attitude towards this criterion is called for rather than a formalistic approach. This includes, for instance, the use of checkboxes. However, some clear limitations are put in place in the Regulation itself: silence, pre-ticked boxes or inactivity do not constitute consent.[106] In relation to smart devices, it is worth pointing out that numerous appliances require access to multiple sources of data. Consequently, the data subject might have to parse through many layers of consent requests before they are able to enjoy their device. If many consent clicks or swipes are required, the consumer's attention is likely to wane. In that way, clicking or swiping fatigue[107] might have detrimental effects on the validity of the given consent.

3. Low-Quality Consent

Asking for the data subject's consent before data processing operations can take place sounds great in theory. However, applying consent in practice often leaves much to be desired. A first problematic hurdle involves the perception that surrounds consent. At present, consumers are often under the impression that the potential risks associated with giving consent are rather low, especially when compared with the benefits that come with such consent. By underestimating potential side effects and elements of misleading conduct, it is currently adequate to speak of *low-quality consent* among smart device users.[108] Beyond the phenomenon of clicking and swiping fatigue, mentioned previously, perhaps the most important hurdle is that consumers refrain from reading privacy policies. Obvious reasons why this is the case include the use of ambiguous or difficult language as well as the overall length of these documents. Thus, in practice, it often happens that consumers consent to the processing of their personal data without fully comprehending the ramifications of this decision. Another element is that privacy policies often fail to appropriately describe what will happen with the collected information (e.g. the data processing policies and retention duration). The consequences here tie in with the previous argument and, again, illustrate the mismatch between what the consumer agrees to and what the data controller or processor does in practice. Even though data processing principles[109] and data subject rights exist in an attempt to remedy this situation, the real-world application of these rights and principles often remains lackluster. Moreover, even if a consumer declines to share certain categories of personal information, undertakings are often still able to draw *probabilistic inferences*[110] from other data collected from that same individual.[111] A final reason why it is appropri-

103 Pagallo, Durante and Monteleone (n 42) 64.

104 Article 29 Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 102) 13–14.

105 Art 4(11), GDPR.

106 Recital 32, GDPR.

107 Article 29 Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 97) 17.

108 Pagallo, Durante and Monteleone (n 38) 64.

109 eg. data minimization, necessity and proportionality.

110 Elvy (n 15) 444.

111 Many data subjects are unaware of what data can reveal about them. Consider, for instance, the ability of a smart TV to infer users' political orientation on the basis of their preference for certain news channels.

ate to speak of low-quality consent is the existence of potential conflicts between different companies that are able to take possession of the collected information. For example: even though company X might have a fair and reasonable data collection policy, if this company subsequently shares collected and processed information with company Y located outside of the European Economic Area, then matters can easily become a lot more complicated.[112]

4. Towards Genuine Informed Consent

It should also be borne in mind that obtaining consent from the data subject is not always necessary. The GDPR sets out a number of lawful processing grounds that have the overall effect of negating the role of obtaining consent.[113] These processing grounds include, inter alia, data processing practices that are necessary for the performance of the contract, to comply with legal requirements or to pursue legitimate interests. Although it makes sense to include additional grounds for lawful processing, questions arise as to the scope of these principles. In the author's view, there exists a genuine risk that companies might attempt to stretch notions such as 'necessary for the performance of the contract' and 'legitimate interests' beyond their acceptable limits. For instance, do legitimate interests include commercial interests such as those inherent to the advertising industry?[114] A preliminary ruling on the scope of interpretation would be welcome at this point and could possibly do away with problems relating to the overly broad interpretation of the lawful processing principles. However, the ECJ has not yet had an opportunity to shed light on the matter.

In an attempt to put consumers back in control of their own data, the author suggests introducing *privacy management dashboards* or consent management platforms.[115] In order to streamline the consent process, a dedicated software tool or an online page could be created where consumers can keep track of all smart devices that are present in their household, see information regarding privacy settings, and modify their consent vis-à-vis the collection of certain categories of personal data. It is imperative that such a digitally designed environment allows for ease of use. To that end, one could think of listing all devices and linking each device's sensors to separate on/off sliders. In doing so, consumers have a 'one-stop shop' for managing their privacy preferences. However, with interoperability often being limited between smart devices, one can immediately counterargue that a one stop shop solution seems more like an idealistic scenario rather than a realistic one.[116]

IV. Technology as a Means to Enhance Privacy and Data Protection

The previous three sections illustrated that, while there is a regulatory framework in place, rules applicable to smart technology offer few incentives for providing *meaningful* transparency and consent mechanisms to consumers. This leads to a rather worrying observation, which forms the premise of the current section. First, it has been established that it is difficult for the average consumer to fully grasp the privacy implications of using smart devices.[117] Second, it was also shown that the average consumer rather easily consents to data processing, even in the face of a low level of transparency.[118] This results in a *consent gap*, i.e. a discrepancy between what the consumer intended to consent to and what he or she actually consented to. This begs the question: is it possible to use technology to our advantage to, at least partially, close this gap? Technical design principles may arguably be used in the context of handling personal data in a way that such data require less protection or even none at all (e.g. by making the end user unidentifiable). While such an approach is far from ideal, it would limit the scope and implications of any given consent and bring consumers' expectations apropos data processing more in line with reality.

---

112 In this regard, see Case C-311/18, *Facebook Ireland and Schrems* [2020] EU:C:2020:559 concerning the framework for lawfully transferring data from the EU to the US.

113 See art 6, GDPR.

114 Irene Kamara and Paul De Hert, 'Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach' (2018) 4 Brussels Privacy Hub 1.

115 Philip Raschke and others, 'Designing a GDPR-Compliant and Usable Privacy Dashboard' in Marit Hansen and others (eds), *Privacy and Identity Management. The Smart Revolution* (Springer International Publishing 2018) 221 et seq.

116 Wolfgang Kerber and Heike Schweitzer, 'Interoperability in the Digital Economy' (2017) 8 Journal of Intellectual Property, Information Technology and E-Commerce Law 39, 42–43.

117 See above at III.3.

118 See above at III.3.

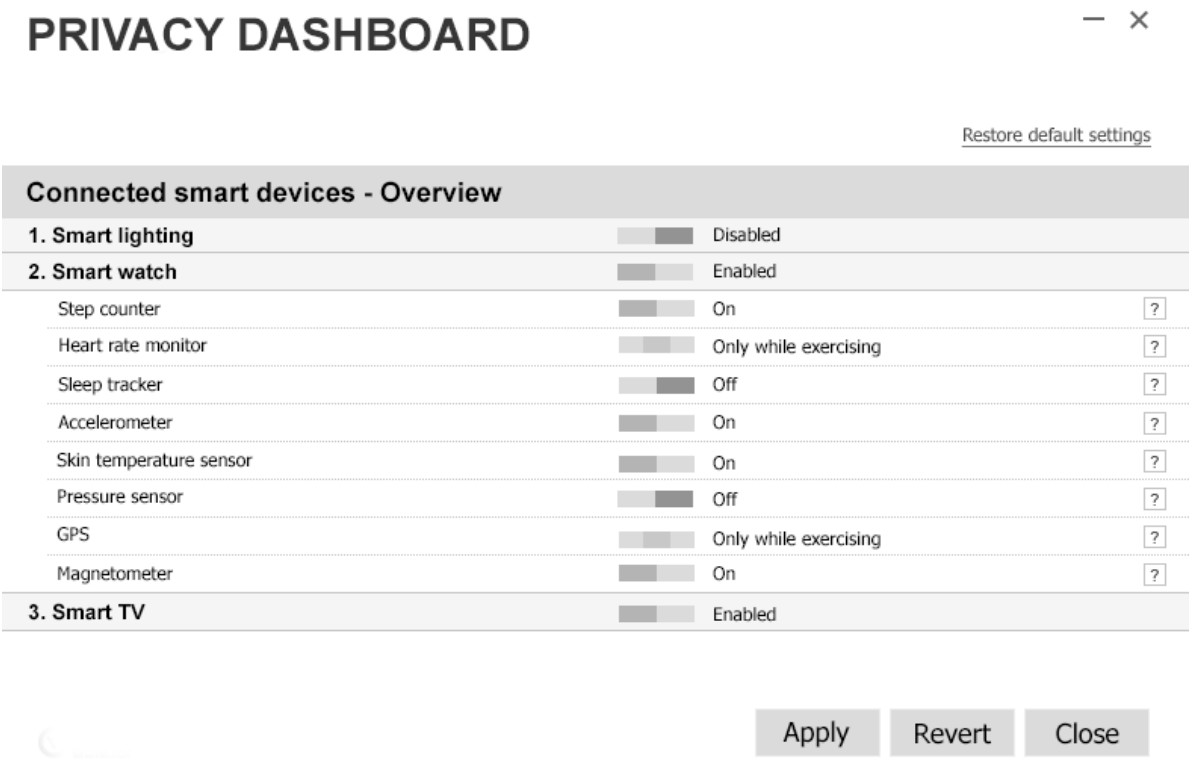

Figure 2 - Overview of what a privacy management dashboard could look like.

A first suggestion in this regard involves putting more emphasis on the role of product design as a means to achieve regulatory compliance. *Privacy by design* (PbD) is often mentioned in this context.[119] Pursuant to this idea, smart device manufacturers need to make sure that data subjects' privacy considerations are taken into account from the product design stage onwards and not merely as an afterthought.[120] From a designer's point of view, putting privacy at the forefront of the product design process can bring clear benefits as retrofitting different privacy design choices on already existing products is often a costly and time-consuming matter.[121] Given that PbD is explicitly included as a requirement in article 25 GDPR, both software and hardware manufacturers will need to consider how to implement and build privacy-friendly features into their devices. At first glance, commendable principles such as data minimization, pseudonymization, and anonymization come to mind when reflecting on PbD. On an abstract level, this implies, among other things, that no more data than necessary are collected. However, in an attempt to leverage these principles into smart environments, practitioners will soon find that it is not an easy task to operationalize PbD. Therein lies the current problem with PbD: proposed solutions often take on the form of abstract or conceptual ideas without specifying practical ways of applying them to real-use cases.

Complementary to design guidelines envisaged by PbD, various *privacy-enhancing technologies* (PETs) are also making their way to smart environments. PETs take matters one step further by acknowledging that a legal or regulatory discourse might not be the most suitable course of action. Instead, they encompass specific technological tools and instruments in view of better protecting privacy. The starting premise for PETs revolves around the idea that the risk of a data leakage or data breach can never be

119 Art 25, GDPR.

120 Pagallo, Durante and Monteleone (n 38) 61.

121 Hervais Simo Fhom and Kpatcha Bayarou, 'Towards a Holistic Privacy Engineering Approach for Smart Grid Systems', *2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications* (2011) 234.

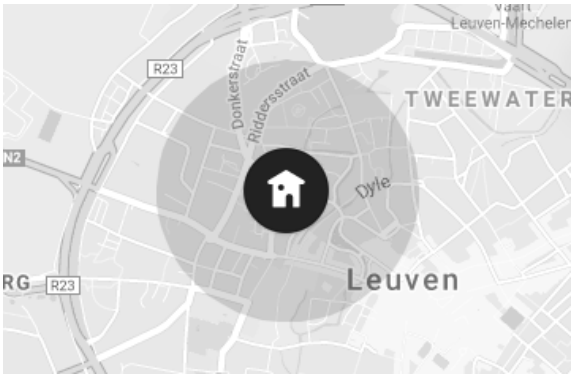

Figure 3 - An example of obfuscation in the context of geolocation data. Instead of processing the exact location of a consumer, only a general indication is given.

completely ruled out and, consequently, that it is better to err on the side of caution.[122] In that regard, PETs are specifically developed to negate some of the effects associated with data breaches.[123] A fitting example of a PET is encryption, which involves using an algorithm to scramble aggregated data into an unreadable format before it is stored in a database (rather than saving data in plaintext in the database).[124] As a result, even if a database were to be compromised by hackers, they would be unable to decipher the dataset without having access to the relevant decryption key. Other popular PETs – such as obfuscation and query enlargement – involve introducing noise (i.e. uncertainty/imprecision) in a dataset.[125] This leads to situations where, for instance, instead of sharing the exact location of a data subject, the data controller only receives an approximation of where the data subject is located.

Neither PbD nor PETs are fully capable of resolving the hurdles that surround transparency and consent in smart environments. However, they do highlight that the rather complex technical nature of innovation instigates a trend to pursue increasingly technical rather than legal solutions to privacy problems. Then again, the shifting sands of technology make it difficult to capture or frame these initiatives in legislation, thereby raising new problems with respect to enforceability. At this point, only time will tell how PbD and PET will evolve. Ultimately, it is plausible that both legal and non-legal stakeholders will have a role to play in shaping the future of privacy in data-driven smart environments.

V. Conclusion

The aim of this article is to put privacy preservation in smart environments into perspective. In recent years, it came to light that consumers are spending increasingly more time in environments that rely on smart devices. While these smart devices offer convenience to end users, they typically come with a privacy price tag. At the outset, this article argued that consumers are often unaware of some of the (detrimental) consequences that smart environments bring about. In view of pursuing a higher level of privacy and data protection for consumers in smart environments, the role of the principles of transparency and informed consent was scrutinized.

Various legal instruments – such as the Consumer Rights Directive, the GDPR, and the ePD – contain extensive transparency requirements, which are specifically geared towards enabling consumers to make better-informed transactional decisions. However, in practice, it remains difficult to apply the principle of transparency to smart environments due to the inherent complexity and rather technical nature of smart devices. Moreover, faced with challenges such as rational apathy and consumer attrition, it becomes apparent that simply providing consumers with more information is not the best course of action. Instead, in an effort to enhance transparency, Section II.4 suggests that inspiration could be drawn from legal design and that it is perhaps necessary to introduce an element of privacy competition between smart device manufacturers.

A second pathway towards an effective level of privacy preservation hinges on the role of informed consent. This article describes consent as the pinnacle of informational self-determination. Yet, when attempting to pursue informed consent in smart environments, several challenges arise. These relate, among others, to a mismatch between the perception surrounding consent and the actual privacy implications of smart technology. Moreover, a number of grounds for lawful data processing exist which – at least partially – hollow out the rationale that underpins the notion of informed consent. On that account,

122 ibid 53.

123 ibid 61.

124 Tamò-Larrieux (n 4) 66.

125 ibid.

Section III.4 took a closer look at privacy management tools and platforms in an effort to remedy these concerns.

On balance, the push for privacy preservation in data-driven smart environments is characterized by steep learning curves and numerous regulatory challenges. A recurring point within this theme is the inherent difficulty of casting appropriate solutions to privacy problems into legislation. Indeed, with the development of technology markets being far from over, attention should be given to risks associated with overregulation: regulators might not only trigger a stifling of innovation, but they could also impede future high-tech development opportunities.

At the same time, the very nature of smart environments adds a new layer of complexity to existing privacy hurdles. As a result, tensions within the existing regulatory framework are palpable and calls for reform are heard. This is especially true in consideration of the current pace of new technological developments. Fortunately, privacy and data protection are gradually attracting more attention from different scholarly angles. Throughout this article, it became apparent that the combination of different perspectives can sometimes lead to new and creative ideas on how to address privacy concerns and that technology can also offer valuable privacy control tools.

From the perspective of the average consumer, the current application of the principles of transparency and consent feels inadequate. On the one hand, consumers are likely to understand and accept that the processing of personal information is necessary in order to make use of particular goods or services. On the other hand, consumers are also entitled to have reasonable expectations regarding the level of privacy offered by those goods or services. Yet, based on the current application of the principles of transparency and consent, it is difficult to argue that these expectations are met. On that note, new approaches to privacy and data protection should be sought after, perhaps in an attempt to do more with less data.