Profiling and targeting users in the Internet of Things - A new challenge for consumer law

Helberger, N.

Published in:
Digital revolution: challenges for contract law in practice

Profiling and targeting consumers in the Internet of Things – A new challenge for consumer law

Prof. Dr. Natali Helberger, Institute for Information Law, University of Amsterdam

I. Introduction

"The door refused to open. It said, "Five cents, please."

He searched his pockets. No more coins; nothing. 'I'll pay you tomorrow,' he told the door. Again he tried the knob. Again it remained locked tight. 'What I pay you,' he informed it, 'is in the nature of a gratuity; I don't have to pay you.'

'I think otherwise,'the door said. 'Look in the purchase contract you signed when you bought this conapt.'

… From the drawer beside the sink Joe Chip got a stainless steel knife; with it he began systematically to unscrew the bolt assembly of his apt's money gulping door.

'I'll sue you,'th door said as the first screw fell out.

Joe chip said, 'I've never been sued by a door. But I guess I can live through it.'[1]

Having a legal debate with one's door sounds very much like a vision from a hopefully very hypothetical future – like the one the science fiction author Philip K. Dick described in his novel. And yet, today, almost 50 years after Dick has first published Ubik, this future does not sound that hypothetical or even far away anymore. This chapter will argue that there is a role for consumer law to make sure that we do not have to have conversations like these with our doors, toasters or other smart appliances in the Internet of Things.

[1] Philip Dick, *Ubik* (Doubleday, 1969) 80-81.

One of the promises of the Internet of Things (IoT) is that everyday appliances, like doors, toasters and fridges will become smart, have some computer-implemented intelligence of their own and are able to communicate. The Internet of Things, sometimes also referred to as the Internet of Objects is "about attaching varying amounts of identity, interaction and inference to objects".[2] "Smart things" or devices are equipped with the ability to collect and process data and interact with other smart things, users but also traders and third parties (insurance companies, governments, advertisers, etc.). These devices are able to take on new functionalities, run applications and provide a platform for (tailored) services and (commercial) communications. Examples are the by now almost proverbial smart fridge that can connect to the local supermarket; smart watches and other fitness devices that monitor users' vital body functions; bottles that notice when they have been opened;[3] smart meters that measure and adjust energy consumption; or smart doors that set the conditions for access, as in the quote above. Insofar, the Internet of Things can revolutionise many aspects of consumers' daily live, but also the very way consumers purchase and use products and services, and engage in their dealings with traders.

Take the example of a smart watch. Equipped with all kinds of sensors, smart watches can track a consumer's steps, the distance walked, the stairs climbed, the calories burned, the routes walked, but also the consumer's heart rate, body temperature, sleep pattern and many others. This information can enable not only companies such as Fitbit, Microsoft or Apple to offer consumers coaching services and (personalised) health and fitness advice. The collected user and usage information can also be shared with insurance companies to adjust the insurance fee;[4] social networks to share personal achievements with friends; advertisers to market new diets or self-awareness services; or governments to monitor the overall fitness of the population. In addition, the smart watch can be directly connected to the smart scale or the smart phone, and maybe soon to the smart fridge or smart cross trainer.

This also means that through the purchase of a smart watch, the consumer does not only acquire a watch. The watch itself is only a tiny part of an entire service universe, and this service university is at least in parts based on the collection of highly individualised data.

[2] Connect Advisory Forum, *Internet of Things: The Next Revolution. A Strategic Reflection About A European Approach to the IoT* (European Commission, 2014).
[3] http://www.cnet.com/news/smart-whisky-bottle-knows-when-someones-been-in-your-stash/ accessed on 15 November 2015.
[4] ATKearney, *The Internet of Things: Opportunities for Insurers* (ATKearney, 2014).

Thanks to the continuous collection and processing of that information, apps and value-added services can be targeted to the needs and preferences of individual consumers.

The question that this chapter will address is what this shift from buying a simple watch to a smart watch, or more generally from buying 'things' to 'smart things' means for consumers and consumer protection law and policy. In so doing, the chapter will focus in particular on the aspect of profiling and targeting in the Internet of Things. Profiling and targeting is a topic that is more commonly associated with data protection law and privacy. This chapter will demonstrate that consumer law, too, will have to play an important role in protecting the legitimate interests of consumers, and guaranteeing a fair balance between consumers, providers of smart things and services, advertisers, insurance companies and other parties.

II. Profiling and targeting consumers in the Internet of Things

The IoT can not only revolutionise the life and experience of consumers. It certainly also revolutionises the way companies can learn about who their consumers are, communicate and interact with these customers. According to an estimate by Cisco, by 2020 fifty billion devices will be connected to the internet. This would translate roughly into 6.58 connected devices per person.[5] The result will be an exceptionally fine-mazed mesh of sensors that surround consumers and can measure any aspect of the consumers' life. Through the ability to turn that information into data, and to combine this data with data available elsewhere, companies will be able to gain completely new, real-time and hyper-personal insights into individual consumers' preferences and behaviours.

Unlike data that is collected about users online behaviour, the data that smart things collect will have its own quality. Such data is potentially far more situational as it is collected by things that surround consumers and are used by consumers in 'real-life' situations. The data is potentially more complete, as at least some smart things can collect that data 24/7. And it can be more easily assigned to a concrete person if the device in question is used primarily by one person (e.g. in the case of a smart watch or a smart phone), whereas computers and portables are potentially used by an entire household. For these reasons, the data collected by smart things is also potentially very useful for manufacturers, service providers but also third parties, such as advertisers, insurance companies or health care providers.

[5] Cisco, *The Internet of Things. How the next evolution of the Internet is changing everything* (Cisco, 2011).

It is not difficult to imagine all the new opportunities to use that information to target consumers individually and provide them with services and products that are specifically tailored to their individual needs and preferences. Profiling and targeting consumers signifies a shift from previous modes of mass communication (advertisements that were "broadcast" to an anonymous mass of consumers) and the mass production of products and services to far more tailored and personalised ways of engaging with customers. And while profiling and targeting is not a development that is restricted to the Internet of Things, the Internet of Things certainly offers particular attractive opportunities for profiling and targeting. Many devices will possess some form of interface and means to communicate with individual consumer, either via the device itself or via connected devices such as smart phones and computers. Consumers can thus be targeted far more specifically and immediately in particular situations, in specific locations or at particular times of the day. And based on the particularly detailed and situational information that can be collected about users and the way they use and interact with smart devices, apps, services and advertisements can be targeted and customised with even greater precision and timing.

A recent study by Cognizant indeed identified the ability to profile and target consumers in the Internet of Things as one of the key trends in the future development and the application of IoT for businesses. Based on the insights from interviews with 200 companies that develop smart products and services, Cognizant found that '[p]roduct data increasingly underpins finer-grain product personalization and richer customer experiences. Smart products reveal insights for remaking how products are built, priced and sold – directly and through channel partners.'[6] Almost a third (28%) of the respondents indicated that they would use the data collected from smart products to personalise products and services (preceded by: automated customer service (40 %), the analysis of product use (39%), sharing the information with suppliers to collaborate on products (32%) and the analysis of a products' life cycle (29%).[7]

The same study also observed that, as a direct consequence, IoT will dramatically change the customer-manufacturer relationship, and introduce far more direct, personalised relationships between manufacturers, service providers and consumers.[8] In other words: consumers do not simply by a product (such as a smart watch). Buying that product is only the beginning of an intimate and potentially long and dynamic relationship with the manufacturer or a network of

[6] Cognizant, *The Rise of the Smart Product Economy* (Cognizant, 2015) 3.
[7] Ibid. 8.
[8] Ibid. 7.

traders and third parties that profile consumers' behaviour and target them with personalised services. Insofar, IoT can affect both, the features and characteristics of products and services, as well as the dynamics between traders and consumers.

These dynamic interactions between traders and consumers can take the form of, for instance, personalised advertising, also referred to as "behavioural targeting" or "Interest based advertising". Commercial messages are tailored to individual consumers, based e.g. on their online behaviour or virtual profiles. It is possible to dynamically adjust prices to certain groups of consumers, individual consumers but also the situation of individual consumers (e.g. air plane ticket prices that go up after a consumer has searched repeatedly for a particular ticket, or charging Mac users higher prices than PC users).[9] Not only prices, but also terms and conditions can be personalised, also in the IoT. Car and health insurance companies, for example, are experimenting with personalised insurance conditions and 'Pay as you drive' or 'Usage based insurance' models.[10] One step further is the use of data analytics and personalised services to actively influence or even change consumer behaviour through personalised nudges.[11]

III. New challenges for consumer law

It probably goes without saying that the massive collection and combination of all sorts of data raises concerns about privacy and the fair processing of personal data and data security. Insofar, when talking about IoT and consumer concerns, data protection and data security are commonly the most prominently discussed concerns.[12] An aspect that has received lesser attention so far are the implications of profiling and targeting in IoT for consumer protection and the application of consumer law, and here in particular the rules about consumer information, contract law and unfair commercial practices.

[9] <http://www.cnet.com/news/mac-users-pay-more-than-pc-users-says-orbitz/> accessed on 15 November 2015.

[10] <http://www.heise.de/newsticker/meldung/Auch-Allianz-plant-Kfz-Tarife-mit-ueberwachtem-Fahrverhalten-2679007.html or http://uk.businessinsider.com/how-the-internet-of-things-is-transforming-the-insurance-industry-2015-7?r=US&IR=T> accessed on 15 November 2015.

[11] *ATKearney* (n 4); Cass Sunstein, *Impersonal Default Rules vs. Active Choices vs. Personalized Default Rules: A Triptych* (Mossavar-Rahmani Center for Business and Government, Harvard, Regulatory Policy Program Working Paper RPP-2012-17, 2012).

[12] Rolf Weber, 'Internet of Things: Privacy issues revisited' (2015) Computer Law & Security Review 618-627; Art. 29 Data Protection Working Party, *Opinion 02/2013 on apps on smart devices* (Art. 29 Data Protection Working Party, 27 February 2013); European Parliament, *Big Data and smart devices and their impact on privacy. Study for the LIBE Committee* (European Parliament, 2015).

Profiling and targeting in IoT affects the way products and services are marketed and advertised, the conditions that are offered, the calculation of prices, and even the question of whether certain consumer (profile)s can access to certain services at all (see section II). These are issues that touch upon acknowledged principles of consumer protection, such as the requirement that consumers are sufficiently informed, the protection of consumers from unfair practices and the maintenance of choice as a basic consumer right. The following section will identify a number of implications from the IoT, and from profiling and targeting in the IoT in particular, for the relationship between consumers and traders, and some of the challenges that flow from this for the application of existing consumer law. It would go far beyond the scope of this contribution to give a complete account of all implications from profiling and targeting in the IoT for consumers. Instead, the next section will focus on three aspects: the shift from off-the shelf to "hyper personal" products and services (section III 1.); the new deal: give data to get service (section III 2.) and the issue of digital market manipulation (section III 3.).

1. From off-the shelf to "hyper personal" products and services

One important implication from IoT, and more specifically from profiling and targeting in the IoT is that consumers purchase not any longer simply an "off the shelf product". Because of the inbuild intelligence products can and will become hyper personal, or as some call it "hyper-relevant" products. This also means that the functionality of a product is not any longer only in the product itself. Instead, the functionality is the result of a complicated web of interrelated apps and services and, ultimately, of the input of the consumer herself. Corresponding to the heterogeneity of the consumer base, each personalised product, or rather "product-service package" is potentially different, and its characteristics can change dynamically over time. What will this mean for the level of consumer protection, and the application of consumer law?

One possible implication will be that many smart devices will fall under a combination of consumer sales law and contract law, but also that consumers, when purchasing and operating a smart device will engage in transactions (be it for money or data) with a variety of players, not all of whom will be known to the consumer. The arising, complex issues of liability and contractual relationships will be treated in another chapter in this book.

Another implication is that each smart product or rather, 'smart product package', will be different, depending on the level of customisation, subscription to value-added services, etc. This may sound trivial but seeing that, as Winn has argued, standardisation is one, if not the earliest form of consumer protection,[13] the buying of smart products will take on an entirely new complexity for consumers. Unlike in situations in which consumers purchase a 'normal dumb' fridge or watch, consumers as well as judges will need to assess smart products not so much as a thing but rather as a platform for value added services, similar to a (mini)computer.

A maybe still somewhat hypothetical but not uninteresting question is to what extent personal relevance and quality of personalisation can become a part of the assessment of the product, and if so, what would that mean for the standard of reasonable expectations as a benchmark? Could I return a smart whisky bottle because it does not give me the serving tips that I like? Or the smart meter because it does not help me to save energy optimally? Personal relevance as quality benchmark of smart devices seems like a notoriously difficult to handle benchmark, not only from the perspective of consumers and providers, but also from the perspective of judges.

2. A new deal: "give data to get service"

One important reason why things in the IoT are smart is that their functionality feeds on a constant flow of usage and user data. In order to be able to provide consumers with real-time feedback on their performance, on the temperature and energy consumption in the house or on the state of maintenance of one's car, devices need to be able to collect and communicate data to the manufacturer or provider of the service. In other words, in order to get functionality consumers need to give data. This also means that consumers no longer simply buy a product in exchange for money. "Paying with your data" will often become part of the deal when buying a smart watch or a smart device. This is data that can be used to enhance the functionality of the service, but also for all other kinds of purposes, such as marketing, profiling, re-adjusting terms and conditions, or reselling and sharing the data. As such, the data can become a commercial asset in its own right. And if some value-added services or apps in the IoT are offered "for free" this is usually not because of the wish 'to do good' but because the IoT offers such excellent opportunities to collect very personal and very accurate data about users and usage.

[13] Jane Winn, 'Information Technology Standards as a Form of Consumer Protection Law' in Jane Winn (ed.) *Consumer Protection in the Age of the "Information Economy* (Ashgate, 2006) 99-120.

There is a growing awareness among policy makers as well as academics that data can become a valuable resource and even a commercial asset in its own right.[14] Only recently, President Angela Merkel called on German consumers to be less protective about their personal data for the sake of the German economy: "Unser Verhältnis zu Daten ist in vielen Fällen zu stark vom Schutzgedanken geprägt (...) und vielleicht noch nicht ausreichend von dem Gedanken, dass man mithilfe von Daten interessante Produkte entwickeln kann. Mit einer falschen Gewichtung entsteht aber auch die Sorge, dass durch Digitalisierung einerseits Arbeitsplätze wegfallen und auf der anderen Seite nicht genügend neue Arbeitsplätze entstehen. Deshalb muss das "Data Mining" (...) die Erhebung und der Umgang mit großen Datenmengen, etwas werden, das sozusagen ein Hoffnungssignal sendet."[15]

In other words, data can turn into a form of (additional) remuneration that consumers are required to pay for services.[16] The European Consumer Commissioner Meglena Kuneva has said already in March 2009: "Personal data is the new oil of the Internet and the new currency of the digital world".[17] "Paying with your data" is an often heard common-place in debates about the new advances of data analytics and the data-driven economy. Services such as Handshake[18] or Datacoup[19] offer brokering services for consumers who want to sell their personal data. And, yet, under European consumer law, the legal implications of the "paying with your data" analogy, and how consumer law can contribute to make sure that "give data to get service" is actually a fair deal are not yet well-understood.

a) Informing consumers about the non-monetary price they pay

Notwithstanding the question of whether it is sensible at all to consider data a price that the consumer pays, it can be stated that *if* the sharing of (personal) data would be part of the 'price' consumers pay for receiving value-added services in the Internet of Things,

[14] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Towards a thriving data-driven economy COM(2014)442 final* (European Commission, 2014); World Economic Forum, *Personal Data: The Emergence of a New Asset Class* (World Economic Forum, 2011).
[15] Angela Merkel, *Rede von Bundeskanzlerin Merkel zur Eröffnung des Zentrums für Forschung und Vorausentwicklung der Robert Bosch GmbH am 14. Oktober 2015* (Die Bundesregierung, 14 Oktober 2015).
[16] Chris Hoofnagle and Jane Whittington, 'Free: accounting for the costs of the Internet's most popular price' (2014) University of California Law Review 606-670; Katherine Strandburg, 'Free Fall: The Online Market's Consumer Preference Disconnect' (2013) The University of Chicago Legal Forum 95-172; Natali Helberger, Lucie Guibault, Marco Loos, Chantal Mak, Lodewijk Pessers, and Bart Van der Sloot, *Digital Consumers and the Law. Towards a Cohesive European Framework* (Kluwer Law International, 2013).
[17] Meglena Kuneva, *Roundtable on Online Data Collection, Targeting and Profiling* (European Commission, 2009).
[18] <http://handshake.uk.com/hs/index.html> accessed on 15 November 2015.
[19] <https://datacoup.com/> accessed on 15 November 2015.

established consumer law principles require that they are informed about this fact. Providing consumers with the information they need to be able to make informed choices has always held a prominent position in European consumer law. According to Arts. 5 (1) (c) and 6 (1)(e) of the Consumer Rights Directive, consumers need to be informed in advance about "the total price of the goods or services inclusive of taxes." Though the notion of price is still commonly interpreted in a sense to refer to the exchange of money, arguably this is bound to change to the extent that in an online environment with its changing business models contracts are increasingly being performed also on the basis of non-monetary exchanges, such as data, but possibly even social capital or attention. One major difficulty in that context is assessing the value of data as a currency. One of the clear advantages of money is that money provides a fairly standardised and transparent way of describing value. It would go beyond the scope of this article to describe the difficulties of attaching concrete value to data.[20] The Consumer Rights Directive foresees in the situation that the price itself cannot be calculated because of the nature of the goods or services,[21] but not in the situation that the price cannot be easily specified because of the nature of the price. Insofar, the Consumer Rights Directive still lacks the necessary instruments to deal with non-monetary forms of remuneration. Having said that, an interesting and often overlooked fact is that with the Consumer Rights Directive, consumer law now at least contains an obligation to inform consumers explicitly about the fact that tracking is taking place, Arts. 5 (1)(g), 6 (1)(r) and Recital 19 of the Consumer Rights Directive, but also, specifically, that communications are personalised.[22] It is also worth noticing that these are obligations that go beyond the level of protection that is offered under data protection law.

Unfair commercial practice law might go further in demanding that consumers are adequately informed, also about non-monetary 'prices' to be paid, or rather: the return-services they are asked to perform (sharing data). An important role of the rules about Unfair Commercial Practices is to create the conditions so that consumers can take better informed decisions on the basis of accurate and well-presented information.[23] Unfair Commercial Practice law could

[20] See insofar *Hoofnagle & Whittington* (n 16); *Strandburg* (n 16).
[21] In which case consumers shall be informed about "the manner in which the price is to be calculated as well as, where applicable, all additional freight, delivery or postal charges", Arts. 5 (1) (c) and 6 (1)(e) of the Consumer Rights Directive.
[22] European Commission, *DG Justice Guidance Document concerning Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights (*European Commission, June 2014).
[23] James Nefh, 'Misleading and unfair advertising' in Geraint Howells, Ian Ramsay, Thomas Wilhelmsson and David Kraft (eds.) *Handbook of Research on International Consumer Law* (Edward Elgar Publishing, 2010) 107-130, 107.

matter for the given context in at least two different ways. For one, one could argue that the material information traders are required to disclose according to Art. 6 and 7 includes information on the price, and that in a digital environment the notion of 'price' must be interpreted broadly, including non-monetary forms of exchanges, such as data, but also attention, intellectual property rights to user generated content, etc. This interpretation is further supported by the qualification in Art. 7(2), namely that a misleading omission can have taken place if a trader fails to identify the commercial intent of the commercial practice (if not already apparent from the context). In particular with the "give data to get service"-deals mentioned above, an underlying and not always sufficiently transparent fact is that the data collected via smart devices will often not only be used to improve the service, etc. but also to monetise that data, share it with advertisers, etc. It is no secret that part of the particular attractiveness of the IoT for the consumer services and products sector is the wealth of information, and potentially very profitable information that can subsequently be commercialised in various manners (re-selling, using for advertising and marketing, etc.). Unfair commercial practice law seems to suggest that where the data is being used not only to provide the service but to extract extra commercial value from that data, and doing so without telling the consumer, can constitute an unfair commercial practice.

The critical question in that context is of course whether the consumer needs that information to take an informed transactional decision, and whether (not) having that information would cause her to take a transactional decision she would not have taken otherwise.[24] This is a difficult and ideally also an empirical question. Much will depend on who in the profiling and targeting context the "average consumer" is. Is that the enlightened, critical digital consumer who is reasonably media literate, aware of the fact that data is streaming and for whom considerations of privacy and information security are important enough to not to buy a product or subscribe a service if her privacy and fair dealings with personal (Big) data is not guaranteed? Or is it a consumer who is primarily interested in the product she is buying, and

[24] It is worth noting that the argument that the exchange of data for service would not constitute a 'transactional decision' in the sense of the Unfair Commercial Practice Directive because that exchange would not affect a consumers 'economic interest' is difficult to accept in an environment in which data is openly described as "the new currency" of a data-driven economy. Here, protecting the privacy and personal data of consumers is clearly not only a matter of "taste and decency" only but also a matter of economic interests that should fall under the ambit of the directive (in favour of a broad interpretation of economic interest also Thomas Wilhelmsson, 'Scope of the Directive' in Geraint Howells, Hans-W. Micklitz and Thomas Wilhelmsson, (eds.) *European Fair Trading Law* (Ashgate, 2006) 49-82, 58.

does not muse about the technical and organisation background as long as the watch (or any other smart device) does what it is supposed to do? We will come back to this question a litter later.

Second, and maybe of even greater practical relevance is No. 20 on the Annex, the black list of unfair commercial practices: "Describing a product as 'gratis', 'free', 'without charge' or similar if the consumer has to pay anything other than the unavoidable cost of responding to the commercial practice and collecting or paying for delivery of the item." Unlike under Arts. 6 and 7, for the application of No. 20 of the Annex it is not relevant if the practice actually has an effect on the consumer's choice and decision to perform a transaction or not. Arguably, the provision is broad enough to also cover the payment of non-monetary forms of remuneration, seeing the lack of a direct reference to notions such as "money" or "price". This interpretation seems to be confirmed by the European Commission itself which, in its guidance on the application of the Unfair Commercial Practice Directive, stated that: "This provision is based on the idea that consumers expect a "free" claim to be exactly that, meaning they receive something for nothing: no money or other consideration has to be given in exchange."[25]

And there are valid reasons to choose such a broader interpretation that also covers the "give data to get service"-deals that were mentioned above. One is, as already mentioned, that personal data will often have a very real economic value to either the provider of a service or application, or third parties, such as advertisers. Insofar, principles of fairness seem to suggest that consumers should be informed about this, or at least not mislead about the fact that they get services "for free". A broad interpretation also avoids a situation that consumers are misled about the fact that they do not owe a service in return, namely the sharing data. Finally, applying No. 20 to also include non-monetary forms of remuneration would have the added benefit of increasing awareness of the economic value of data for both, consumers as well as traders. It could be an important means to re-establish the balance between consumers and traders in a digital, data-driven environment.

b) About the fairness of "give data to get service"-deals

Another question is to what extent "give data to get service"-deals should be a matter for scrutiny under unfair contract terms regulation. The objective of contract law and the

[25] European Commission, *Commission Staff Working Document. Guidance on the Implementation/application of Directive 2005/29/EC on Unfair Commercial Practices* (European Commission, 2009).

Directive about Unfair Terms in Consumer Contracts[26] is to promote fairness and the balancing of rights and obligations, especially in situations in which the consumer is in a weaker negotiation position (such as in the case of standard form contracts). Even if one does not consider data as (part of the) price that consumers commit to pay or even denies a typical 'economic' interest, still contract law can have a role to play. As Wilhelmsson and Willet explain convincingly fairness rules in contract law can also be used to support other societal policies or entitlements from fundamental rights.[27] Fundamental rights, too, can have a role in the weighting process, even though, as Collins points out, it might be necessary to translate e.g. the constitutional conception of privacy into a concept that fits better the realities of a relationship between private actors (rather than the state-citizen relationship).[28] So, if the Unfair Terms in Consumer Contracts Directive declares that a contractual clause "shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer" (Art. 3(1) of the Unfair Terms in Consumer Contracts Directive), that provision is arguably open to a broader interpretation, considering also other than the 'typical' consumer interests, including interests of privacy and the protection of personal data, freedom of expression and protection from the chilling effects that surveillance might have.[29]

For example, if an insurance company does make the height of the insurance fee dependent on the willingness to agree to tracking and data sharing, or if providers of smart meters reserve the right to share the collected data with third parties, such as advertisers or environmental agencies, could that create a significant imbalance in the parties rights and obligations? Particularly when taking into account that the sharing of energy consumption information with advertisers is not necessarily in the interest of consumers? Receiving targeted advertising may not be the primary purpose why consumers would buy a smart

[26] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, Official Journal L 095 , 21/04/1993 P. 29 – 34.

[27] Thomas Wilhelmsson and Chris Willet, 'Unfair terms and standard form contracts' in Geraint Howells, Ian Ramsay and Thomas Wilhelmsson (eds.) *Handbook of Research on International Consumer Law* (Edward Elgar, 2010) 158-191, 159-160. This is not the place to discuss the general positions on contract law on whether fairness considerations or considerations of party autonomy should serve as a point of departure. While in some countries there seems to be a focus on fairness considerations in others, particularly in common law countries, party autonomy may trump, *Wilhelmsson and Willet 2010*, ibid.

[28] Hugh Collins, *Utility and Rights in Common Law Reasoning: Rebalancing Private Law Through Constitutionalization* (LSE Law, Society and Economy Working Papers 6/2007, London School of Economics and Political Sciences, 2007), 19.

[29] See more generally on the threat of interference and possible implications for freedom of expression, European Court of Human Rights, Altuğ Taner Akçam v. Turkey, no. 27520/07, § 81, 25 October 2011.

watch. And for some consumers, notably the less affluent ones, such a deal could create additional pressure to forsake their privacy in favour of a better deal.[30] Under such circumstances, does the obligation to share data that is collected by smart devices pose an undue burden for the consumer?

Relevant factors to consider in that assessment[31] could be e.g. the extent to which consumers are able to safeguard their own interests and bargain for fair deals, including the level of transparency provided;[32] the reasonable expectations of consumers but also the availability of choice in the form of either alternative or competing offers; the overall (substantive) fairness, but also the compatibility of certain terms and conditions with other rights and freedoms of consumers, such as the right to privacy. Wilhelmsson and Willet, for example, mentioned as an example of particularly problematic terms those that ”impact the private sphere of life and cause losses that consumers may find […] particularly difficult to absorb.”[33] Applied to the given case this could mean that terms that require consumers to share information not only with the provider of an app or service but with third parties that may or may not be affiliated with that party could be potentially unfair, for example if that means that consumers would as a consequence lose control of that data and could not prevent its abuse, or if the obligation would run counter to the consumers' rights under data protection law. In most cases, consumers will not even be able to understand fully the implications, seeing the complexity of the value chain and the underlying technical issues. Another reason to be particularly vigilant about "give data to get service"-deals is the difficulty, not only for consumers, to assess the real "costs' of this form of data sharing for consumers. As mentioned earlier, it is very difficult or even impossible to attach concrete costs to data. Equally difficult it is to assess the consequences when such data is being released, and whether it may lead a second or even third life on its own (without the user directly benefiting) or is used to take any decisions that disadvantage the consumer (e.g. higher insurance feeds). The difficulty of developing a concrete measurement or benchmark of when the amount of data requested is

[30] Which was also one of the reasons why in the Netherlands, the insurance company Achmea has been recently nominated for the "Big Brother Award", an annual award that is 'won' by the person or entity with the biggest privacy sins.

[31] Which can also depend on the country in question, compare *Wilhelmsson and Willet 2010* (n 27).

[32] Chris Willett, *Freedom in Consumer Contracts: The Case of Unfair Terms* (Ashgate, 2007), 17.

[33] *Wilhelmsson and Willet* (n 27), 162. See also Willett: "An important aspect of the idea of fairness/protection of consumer interests in the context of consumer contracts seems to be the idea that consumers enter contacts in order to sustain and enhance the private sphere of life, rather than to make a profit. The terms of these contracts therefore affect the physical safety, proprietary, economic and social interests arising in, and affecting, the private sphere of life." *Willet* (n 32), 37.

out of proportion or "too expansive" when compared to what users get in return is of course also a challenge when applying the fair balancing test to "give data to get service"-deals.

Relying here on market forces to determine an adequate price (as suggested, though in a different context, by Willet)[34] is little helpful, as traditional market mechanisms do not work in determining the right price or value of personal data.[35] Rather, the overall picture will need to decide, e.g. whether the data in question is sensitive or not (with the result that it merits stronger protection, e.g. under data protection law); whether it is being shared with third parties or not; the risk of privacy breaches and security threats; the amount of data being collected; as well the way and the purposes for which it is being used (e.g. to further the interests of the consumer, vs. the interest of an insurance company or advertiser), but also the utility that consumers get in return. In other words, it could very well be that the fact that the consumer is required to share date is being outbalanced by the added utility that she receives from that service. Vice versa, there are situations in which the sharing of data has the potential to lead to consumer detriment, algorithmic discrimination or other forms of unfavourable decision making. Here, the assumption of contractual unfairness lies closer at hand.

Another interesting question is to what extent certain forms of "nudging" or personalised advertising with the goal of convincing the user to actually enter into the contract could have for the assessment of fairness. Thal, for example, suggests two situations in which it can be concluded that the bargaining power is not equal (which could be an indicator of contractual unfairness): the situation of monopoly power with the consequence that the other party, typically the consumer, has no choice, and a situation in which the other party is particular weak.[36] Possible sources of weakness can be, according to Thal, ignorance, necessity or, quite interestingly, trust.[37] In an age of Big Data and algorithms, a fourth possible source of weakness can arise: which is susceptibility to digital market manipulation (more about this in the next section)

3. Digital market manipulation

It was mentioned earlier that IoT facilitates the collection of detailed information about the user, and the creation of user profiles. That knowledge can be use, to improve the

[34] *Willet* (n 32), 52.
[35] *Strandburg* (n 16).
[36] Spencer Nathan Thal, 'The inequality of bargaining power doctrine: the problem of defining contractual unfairness' (1988) 8 Oxford Journal of Legal Studies 17-33, 29.
[37] Ibid, 32.

communication with the consumer, to target messages more effectively and customise products and services. The deepened knowledge about the user, however, can also be used to identify personal biases and weaknesses. Hanson and Kysar describe this as an entirely new source of market failure.[38] They explain: "Rather, it is that manufactures have incentives to utilize cognitive biases actively to shape consumer perceptions throughout the product purchasing context and independently of government requirements. Advertising, promotion and price setting all become means of altering consumer risk perceptions".[39]

Kaptein et.al referred in this context to "persuasion profiles": "sets of estimates of the effectiveness of particular influence strategies on individuals, based on their past responses to these strategies".[40] Different people respond to different triggers, and knowing these can help third parties, such as advertisers or marketers to deploy a persuasion strategies. Some people are more perceptible to recommendations by friends, others to recommendations by experts. Some prefer short texts, others long, some respond to negative, others to positive framing. Similarly, different people exhibit different biases and irrationalities, and again, data analytics, profiling and targeting allows to uncover these and exploit them to the advantage of advertisers, firms, etc..[41] If studies find that women tend to feel less attractive on Monday mornings, this is useful information for advertisers of beauty products.[42] If predictive profiling makes it possible to predict which people are likely to cancel a subscription, this is valuable information for service providers' strategies to prevent them from switching to a competitor.[43] Profiling and targeting in the IoT adds an additional dimension to this because of both, the ability to collect even more detailed and situational data on the consumer, and to targeted the user context- and situation-specifical.

[38] Jon Hanson and Douglas Kysar, 'Taking Behaviouralism Seriously: Some Evidence of Market Manipulation'(1999) 112 Harvard Law Review 1564-1565; Jon Hanson, and Douglas Kysar, 'Taking Behaviouralism Seriously: The Problem of Market Manipulation' (1999) 74 New York University Law Review 630-749.

[39] *Hanson and Kysar 1999*, ibid. 637.

[40] Maurits Kaptein, Dean Eckles, and Janet Davis, 'Envisioning Persuasion Profiles: Challenges for Public Policy and Ethical Practice' (2011) 9/10 Interactions 66-69, 66; also: Maurits Kaptein, Joyca Lacroix and Privender Saini, 'Individual differences in persuadability in the health promotion domain' in Thomas Plough, Per Hasle and Harri Oinas-Kukkonen (eds) *Proceedings of 5th International Conference on Persuasive Technology: PERSUASIVE 2010* (Springer, 2010) 82-93.

[41] Ryan Calo, 'Digital Market Manipulation' (2014) 82 The George Washington Law Review 995-1051, 1003.

[42] Rebecca Rosen, 'Is this the Grossest Advertising Strategy of All Time?' (2013) The Atlantic. 2013 < http://www.theatlantic.com/technology/archive/2013/10/is-this-the-grossest-advertising-strategy-of-all-time/280242/> accessed 10 October 2015.

[43] Eric Siegel, *Predictive Analytics: The Power to Predict Who Will Click, Lie, or Die* (John Wiley & Sons, 2013), 6-7.

There is a very fine line between informing, nudging and outright manipulation. And one, or maybe even one of the main challenges for consumer law and policy in the context of profiling and targeting in the Internet of Things is to identify and delineate where exactly this line runs.

a) The Unfair Commercial Practice Directive as point of departure for the conceptualisation of fairer marketing practices in the Iot

Much of the normative discussion about profiling and targeting consumers in the IoT, and certainly the topic of digital market manipulation, is about the need to find a proper balance between the interest of industry to engage in new forms of marketing and product development, and the autonomy and free choice of consumers. Digital market manipulation cuts right into this delicate balance, exactly because of the persuasive and pervasive potential of personalised communication. The Unfair Commercial Practice Directive will have an important role to play in providing guidance on what fair algorithmic marketing practices are, in the IoT, and beyond.

Central to the directive's objective is the autonomy of the consumers' decision making process, through protection against deception and unfair restrictions of consumer choices. Consumers may not be 'mislead or exposed to aggressive marketing" and any claim made by traders in the EU should be "clear, accurate and substantiated, enabling consumers to make informed and meaningful choices".[44] The making of autonomous, free and not unfairly manipulated choices is thus a central point of attention for the directive. But the provisions about unfair commercial practices are particularly interesting for two additional reasons.

One is that the rules about unfair trading, including those in the Unfair Commercial Practice Directive, do not exclusively take the interests of the individual consumer as point of departure. This is interesting and relevant because profiling and targeting consumers in the IoT does not only touch upon issues of individual consumer protection. It also touches upon broader, more conceptual questions about the kind of information economy we would like to live in, and the values that should shape it. Fairness, privacy, autonomous choices may be important rights or entitlements of individual consumers/citizens, but they are also the quintessential building blocks of a free digital society. And since much of the interactions within the digital society are being privatised and commercialised, it is difficult to separate the individual from the societal perspective entirely. It appears that the provisions about

[44] *European Commission 2009* (n 25), 6.

Unfair Commercial Practices provide at least some room to also consider broader societal implications of unfair marketing practices, even if those broader societal issues are still primarily viewed through the lens of the consumer as economic decision maker.[45]

The other is that the protection of privacy concerns more specifically is not alien to the provisions about unfair commercial practise. From the way that the rules about unfair commercial practices, coercion and harassment have been applied to situations of door step selling or phoning people at their homes speaks a respect for the personal autonomy and privacy of consumers.[46] That the provisions about unfair commercial or unfair trading practices can play an important role in protecting also the privacy of consumers is even more established in the US. The Federal Trade Commission, the American Consumer Protection and Fair Trade Authority has played over the past years an important role in furthering consumer privacy. The fair trading law's rules about deception and fairness have played a prominent role in this. As the US scholars Solove and Hartzog argue in a recent article, "FTC privacy jurisprudence has become the broadest and most influential regulating force on information privacy in the United States — more so than nearly any privacy statute or any common law tort".[47]

b) Targeting & profiling in the IoT as an aggressive practice

The rules about unfair commercial practices do not only protect the interest of the consumer in being properly informed (see insofar section III 2). They also embrace a broader understanding of fairness in commercial transactions against practices that violate more vigorously the autonomy, freedom to choose, and arguably also the privacy and dignity of consumers.[48] As Howells argues, a central element of the provisions about aggressive practices is the impairment of the consumer's freedom to choose, though, as he also points out, the line between advertising as in essence a form of persuasion, and exercising undue influence or even coercion can be very thin.[49] And yet, as vague as the notion of "aggressive

[45] *Wilhelmsson* 2006 (n 24), 63; *European Commission* 2009 (n 25) (concentrating primarily on the case of environmental concerns), 37-46; Chris Willet, 'Fairness and Consumer Decision Making' (2010) 33 Journal of Consumer Policy 247-273.

[46] Geraint Howells, 'Aggressive Commercial Practices' in Geraint Howells, Hans-W. Micklitz and Thomas Wilhelmsson (eds.) *European Fair Trading Law* (Ashgate, 2006) 167-195, 178; Geraint Howells, Hans-W. Micklitz and Thomas Wilhemsson, 'Towards a better understanding of unfair commercial practices' (2009) 52 International Journal of Law and Management 69-90.

[47] Daniel Solove, and Woodrow Hartzog, 'The FTC and the New Common Law of Privacy' (2014) Columbia Law Review 584-676, 583.

[48] *Compare Howells 2006* (n 46) 167-168.

[49] Ibid, 168.

practice" is it is easy to see its relevance for the topic at hand, and in particular for the matter of "digital market manipulation".

Take the example of an advertiser who, thanks to the constant transfer of personalised information learns that a consumer has just stepped from the scale three kilo's heavier. The advertiser seizes the opportunity to target her with advertisement for a new, rather expansive diet coaching service that is exactly tailored to her personal level of fitness and weight. Insensitive but perfectly legitimate advertising or aggressive commercial practice? In order to be an aggressive practice the showing of the targeted advertising would need to comply with the three requirements of Art. 8 of the Unfair Commercial Practice Directive (respectively the national rules implementing it): it would need to constitute a form of harassment, coercion or undue influence; it would need to (or be likely to) impair the consumers freedom of choice or conduct; and it would need to (or be likely to) cause a transaction that the consumer would otherwise have not taken.

aa) Targeted advertising as harassment, coercion or undue influence

Though it seems not always easy to draw a clear line between harassment, coercion and undue influence, there seems to be some agreement that harassment is concerned also and particularly with commercial practices that invade the private space of the consumer.[50] Possible examples are doorstep selling or phoning or emailing the consumer at her home.[51] These practices force the consumer to engage with the trader within the confines of her private sphere (home), where the consumer may be less alert and less trained to defend herself against unfair practices than e.g. within the setting of a shop. If phoning and mailing the consumer in her house can already be seen as a potentially unfair invasion of the private sphere of the consumer, arguably, sending advertising to devices that directly surround the consumer in her private sphere could, under circumstances, be considered harassing as well (and provided the other conditions of Articles 8 and 9 of the Unfair Commercial Practice Directive are complied with). This is even truer for communication that is delivered to devices that the consumer carries close to her body, such as reaching out to her over her smart phone or smart watch.

But it is not only the location that matters, timing matters as well (Art. 9 (a) of the Unfair Commercial Practice Directive). The Internet of Things is 24/7 and gives marketers the opportunity to target consumers at any moment of the day, including in the early hours in the

[50] *Howells, Micklitz and Wilhelmsson 2009* (n 46) 76.
[51] *Howells 2006 (n 46)* 179, 182.

privacy of one's bathroom, when the consumer has just stepped of the scale and discovered she has gained a couple of kilos.

Profiling and targeting the consumer could, under certain conditions, also amount to coercion. Obviously it is less the exercise of physical power, and more the exercise of psychological power that would be at play here. Because, as a result of profiling and data analysis, advertisers and service providers are able to identify not only personal preferences, but also possible biases and weak spots in the consumer, this does give room to also play on the consumer's emotions and fears, such as the fear of gaining weight.

The detailed knowledge about the consumer could, finally, also place traders into a position of power, in the sense of the directive's definition of "undue influence". According to Art. 2(j) of the Unfair Commercial Practice Directive undue influence is defined as the "exploiting a position of power in relation to a 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". According to Howells this can include situations in which the trader has the power to persuade the consumer, either because the consumer depends on the cooperation of the trader, or because the trader has at his disposal psychological tools to sway the consumer into the making of a transaction.[52] The detailed knowledge about the consumer's personal situation, her preferences, fears and biases can form a potentially effective source of persuasive potential. As has been explained above, the entire purpose of making and using persuasion profiles is to find the right "persuasion" strategy for each consumer, based on her characteristics and persuasion potential. The difficult question is to decide where the limit lies between legitimate, albeit technologically sophisticated persuasion and the exercise of undue influence.

One important factor in this context could be the knowledge of the user of the fact that she is being persuaded, based on her persuasion profile, because only with such knowledge she is actually able to mobilise her defence strategy, should she wish to do so. Another important factor could be her ability to opt out of targeted messages, as a means to restore the imbalance in control power between user and trader. An interesting question would be to what extent the amount of information collected about the consumer, or the sensitivity of that information could play a role in the assessment. More generally, useful insights for the

[52] *Howells 2006* (n 46) 188; Reiner Schulze and Hans Schulte-Nölke, *Analysis of National Fairness Laws Aimed at Protecting Consumers in Relation to Commercial Practices* (Report Commissioned by the European Commission, DG Sanco, 2003), 37.

assessment could be derived from the ongoing discussion about the ethics of persuasion and nudging),[53] though it exceed the scope of this contribution to go into more depth into this strand of analysis.

bb) Impairment of the freedom of choice

And then there are of course the conditions in the Unfair Commercial Practice Directive itself. The practice is only unfair if it impairs the consumer's freedom of choice or conduct and causes her to make a transaction that she would have otherwise not taken. Under which conditions profiling and targeting can amount to significantly impairing (or being likely to impair) a consumer's freedom of choice or conduct will depend on the persuasive potential of the personalised message and the extent to which the practice reduces the autonomous decision making process.[54] This is a difficult and also empirical question. So far, research on the effects of personalised communications in general is still a developing area of research.[55] Answering the question will require deeper understanding of how exactly profiling and targeting affects the choices of consumers in an individual case, or: to use the wording of the directive: "taking account of all its features and circumstances" (Art. 8 of the Unfair Commercial Practice Directive). For example in the case of the above mentioned example – a consumer is being targeted with diet products after she has learned from her scale that she has gained a couple of kilo, it would be necessary to better understand how deep the fear of gaining extra weight is (is she obese or bulimic , over-or normal weighted, what is her age, does she have a history of (unsuccessful) dieting, etc.), how perceptive to personalisation strategies, how much the timing of the message plays a role etc. It is important to keep in mind, however, that an important purpose of targeted advertising is to be better able to effect a change of behaviour in consumers, and increase the likelihood of the consumer purchasing a product or service.

[53] Andreas Spahn, 'And Lead Us (Not) into Persuasion…? Persuasive Technology and the Ethics of Communication' (2012) Sci Eng Ethics 633-650; Peter-Paul Verbeek, 'Persuasive Technology and Moral Responsibility. Toward an ethical framework for persuasive technologies' (2006) Persuasive 1-15.

[54] An interesting question in this context is to what extent the directive would apply to practices that trigger not the consumer's rationality but her automatic behaviour (such as e.g. defaults do).

[55] Laura Brighta and Terry Daugherty, 'Does customization impact advertising effectiveness? An exploratory study of consumer perceptions of advertising in customized online environments'' (2012) Journal of Marketing Communications 19-37; Jason Jensen, Andy King and Nick Carcioppolo, 'Why are tailored messages more effective? More Effective? A Multiple Mediation Analysis of a Breast Cancer Screening Intervention' (2012) Journal of Communication 851-868; Richard Petty and John Cacioppo, *Communication and persuasion: Central and peripheral routes to attitude change* (Springer, 1986).

cc) Causing a transactional decision that the consumer would not have taken otherwise

This observation is also relevant for the next criterion: causing the consumer to take a transactional decision that she would not have taken otherwise. Again, much will depend on the actual persuasive potential of the personalised communication. An added difficulty in this context is that because the message has been personalised to the individual situation and preferences of an individual, arguably the likelihood is greater that the consumer already had a predicament for taking that particular decision, because it corresponds with her individual needs and preferences. The challenge for the consumer, in the case of individual consumer redress (to the extent that national laws foresee in this possibility), would then be to demonstrate that even though the personalised communication does communicate with individual needs and preferences, the consumer was determined not to enter into that transaction (e.g. order diet products), and was only swayed because of the personalised nudge to decide differently.

c) The quantified consumer – empowered or vulnerable

Much will of course depend on who the "average" consumer of personalised IoT products and services is. The average consumer, as the 'reasonably informed, observant and circumspect' consumer,[56] is an important benchmark for the application of the Unfair Commercial Practice Directive's provisions (Recital 18 of the Unfair Commercial Practice Directive). Arguably, the requirements for the average consumer in a digital environment must reflect in some way or other the greater technical and organisational complexity but also the changed nature of digital or digitally-enhanced products, and hence her ability to deal with that complexity. For example, the buyer of a smart watch will need to have a different level of media literacy, technical understanding but also understanding of the basic legal implications than the buyer of a "normal" analogue watch. Otherwise it is difficult to understand how she can correctly assess the functioning but also the implications of her choices, for example for the privacy and safety of her personal data.

This leads to the question: who is the "average user" in the IoT? Is this the technically sophisticated, media literate consumer? The concept of the Internet of Things is inevitably connected to the notion of the quantified self – a notion, or rather a movement, coined by the editors of the tech-magazine Wired, Gary Wolf and Kevin Kelly. Quantified self, or as the movement describes itself "self-knowledge through numbers"[57] refers to the idea that digital

[56] CJEU 16.07.1998 Case C-210/96 (Gut Springenheide) ECR 1998 I-4657.
[57] <http://quantifiedself.com/> accessed on 15 November 2015.

technologies also allow users to track themselves, thereby better get know to know their body, mind, environment and behaviour.[58] Users can also use the data they collect about themselves for self-improvement: becoming more efficient, healthier, productive, social, etc. Insofar the Internet of Things may bring consumers one giant leap closer to the notion of informed consumer in the sense that consumers get to know themselves better, their preferences and needs.[59]

At the same time, it is also exactly this complexity of the technical environment and value chain, the lack of benchmarks of similar "standardised" analogue products and the opacity of the underlying processes that challenge the ability of the digital consumer to navigate digital product markets in the IoT; and make her potentially more perceptive to practices such as digital market manipulation. If one defines "vulnerability" as the "limited ability to deal with commercial practices"[60] one may even wonder at which point digital marketing practices, and in particular if they are based on intrinsic data analysis, opaque algorithms and sophisticated forms of persuasion, turn the normally "average" consumer into a vulnerable one. So while it may be that the quantified consumer is technologically more sophisticated and empowered, it is similarly possible that as the "profiled consumer" she is also more credulous and defenceless against new, more sophisticated forms of personalised marketing in the Internet of Things. This could be an area that merits more legal-empirical research.

IV. Conclusion

This chapter has pointed to some of the possible challenges from the Internet of Things for the "profiled consumer". These challenges go beyond issues of privacy and data protection – which will continue to play a prominent role. In addition, the protection of contractual fairness, adequate information and autonomous and free choices comes to the fore. Particular attention has been payed to the issues of "free services" and "give data to get service"-deals, as well as practices of digital market manipulation. It has been argued that unfair commercial practice role will have a prominent role in ensuring fairness in the dealings between consumers and traders in the Internet of Things.

[58] Deborah Lupton, *Self-tracking cultures: towards a sociology of personal informatics' ACM, Proceedings of the 26th Australian Computer-Human Interaction Conference: Designing Figures, the Future of Design, 2-5 December 2014* (University of Technology Sidney, 2014).

[59] A question for future research could be to what extent self-tracking and digitally enabled self-improvement could have on the concept of the "informed consumer" and the idea of the consumer as an autonomous economic actor.

[60] Bram Duivenvoorde, 'The protection of vulnerable consumers under the Unfair Commercial Practice Directive' (2013) 2 Journal of European Consumer and Market Law 69-79, 73.

This is not to say that consumer law, and the Unfair Commercial Practice Directive in particular, are the optimal or last answer to the consumer protection challenges from profiling and targeting consumers in the Internet of Things. The strong focus on economic interests and the fact that societal interests are primarily viewed through the lens of a consumer who is about to take an economic transaction; the fact that economic transactions are still primarily considered transactions for money, not data; the requirement of an effect on a transactional decision, which is limited helpful in situations in which consumers are largely ignorant or do not feel they have a choice and take the decision anyway; and the fact that the directive describes which practices are unfair, rather than giving guidance on what fair media practices are – these are just some of the limitations that the application of consumer law, and unfair commercial practice law, to the Internet of Things encounters.

And yet, consumer law and the provisions about unfair practices can provide a new and inspiring perspective for thinking about the protection of the "profiled consumer" in the Internet of Things. They could form the point of departure for a broader discussion on what fair marketing practices are in the context of profiling and targeting, in and beyond the Internet of Things. They could even contribute to the protection of consumers' privacy. Insofar, this chapter has also touched upon the question of how data protection law, privacy and consumer law could complement each other, and pointed to some relevant questions for further research.