Is all fair in war against unhealthy and unsustainable lifestyles?

The right to privacy vs. modern technology in consumer contracts

Joasia Luzak*

Abstract

In their quest to curb unhealthy and unsustainable consumer lifestyles, policymakers may be tempted to use modern technology to nudge consumers to conclude only the 'right' contracts. However, this would create a tension between individual consumers' autonomy and their fundamental rights, and public interests in safeguarding consumer welfare and environment. Rather than discussing restrictions of autonomy that may occur as a result of nudging, this chapter focuses on dangers to the protection of fundamental rights in the regulation of consumer contracts in the food and textile industry sector. It considers to what extent the (European) legislators guarantee European consumers' constitutional right to privacy in light of technological developments that could be used to nudge consumers to choose healthy and sustainable lifestyles. The right to privacy may become a victim of the fight for better consumer lifestyles, when policymakers and traders support the use of modern technology, without introducing a well-thought-out regulation thereof. This chapter argues that since modern technologies are constantly developing, policymakers should keep a close vigil over them and not be afraid to introduce rules that would ensure consumer data safety and security.

1 Introduction

Overweight and obesity concern about 67% of men, 57% of women, and more than 25% of children in the UK[1] and cause a serious public health problem in Europe[2]. Policymakers often perceive the modern lifestyle as the cause of the growing number of overweight and obese people; with sedentary work environment, cheap and easily available processed food, consumers receive more energy intake, while spending less thereof[3]. Modern lifestyles demand also that consumers follow fashion choices and consume more clothing than is necessary due to their wear-and-tear. Increased consumption and demand for textile products dictate a more efficient and faster production line, which may negatively impact the supply chain of fashion companies, as well as working conditions within it[4]. Food and textile industry provide, therefore, examples of consumer products' sectors, which policymakers may want to regulate, among other things, in order to ensure that consumers receive healthy and sustainable products. The difference between these sectors is that to reach this goal, food and health policies, in principle, would focus on the wellbeing of consumers themselves, while policies in the textile industry would mostly concern wellbeing of workers in the industry, as

* Dr. Joasia Luzak, Associate Professor, University of Exeter Law School. External Researcher Fellow at the Centre for the Study of European Contract Law, University of Amsterdam. Member of the Ius Commune Research School. The author would like to thank C. Mak and R. Edwards for their valuable comments regarding an earlier version of this paper.

[1] See, in particular, Boseley (2014) and Knapton (2016).

[2] For details see European Commission (Eurostat).

[3] For details see EHLA (European Healthy Lifestyle Alliance).

[4] See, in particular, Danyliak (2015) and European Parliament (2014).

well as the protection of the environment. The commonality of these two sectors is that policymakers attempt to influence consumer behaviour in them through contract law measures. To curb unhealthy and unsustainable consumer lifestyles, European and national policymakers invest thus more in research and public policy campaigns, to find out what impacts consumer decision-making and how to influence it[5]. That is to say, how to nudge consumers to conclude only the 'right' contracts[6].

Scholars have been debating the validity and the effectiveness of nudges, concerned with the need to preserve the main principle of contract law: parties' autonomy[7]. Nudging, e.g., through choice architecture, could obstruct consumers' free will in what contracts, and on what conditions, they conclude[8]. The policymakers' intervention could, furthermore, not only negate contractual principles, but also infringe consumers' constitutional rights, such as the right to privacy. There is clearly a tension between individual consumers' autonomy and their fundamental rights, and public interests in safeguarding consumer welfare, environment, sustainable working conditions, etc. While the goal of policymakers to help consumers help themselves seems laudable[9], it raises a question whether this goal should be achieved by employing any (technological) means, especially, if these could infringe on consumers' constitutional rights, like the right to privacy. Rather than discussing restrictions of autonomy that may occur as a result of nudging, this chapter focuses, therefore, on dangers to the protection of fundamental rights in the regulation of consumer contracts. This chapter considers to what extent the (European) legislators guarantee European consumers' constitutional right to privacy in light of technological developments that could be used to nudge consumers to choose healthy and sustainable lifestyles.

Paragraphs two and three set the scene for this research, outlining the battlefield. That is to say, they illustrate the friction between the use of technology to nudge consumers towards the 'right' choices and consumers' rights to privacy. Paragraph two presents what strategic policy objectives policymakers may have in encouraging healthy and sustainable consumption, while paragraph three illustrates how these objectives may clash with constitutional and contractual rights and principles, specifically the right to privacy and consumer autonomy. Paragraph two emphasises the importance given by policymakers to changing unhealthy and unsustainable consumer habits. It shows that policymakers may be tempted to allow the use of modern technological developments without much regulatory oversight, if empirical research could prove that their use would be effective and efficient. Two types of policy interventions distinguish themselves in this respect and will be discussed: measures supporting informed consumer choice and measures aiming to change the market environment. Regrettably, policy measures that are effective in combating unhealthy consumer choices, may nonetheless, simultaneously, infringe consumer autonomy and privacy. To determine whether this may indeed be the case, paragraph three clarifies existing European

[5] See specific examples thereof discussed further in this chapter.
[6] On increased consumer awareness of corporate social responsibility issues see, in particular, Niemtzow (2013) and European Commission (2013). On various awareness campaigns to encourage healthier food habits, see, in particular, EATWELL (2013), pp. 24-29 and Oliver and Ubel (2014), p. 333.
[7] See, in particular, Alemanno and Sibony (2015).
[8] See, in particular, Carolan and Spina (2015), pp. 161-178.
[9] Even though nudging as a form of soft paternalism has its staunch critics, as well, see, in particular, Waldron (2014).

protection of consumer privacy, functioning on the basis of Data Protection Directive[10] and ePrivacy Directive[11], which introduced a ban on collecting data that could identify consumers. The question arises whether modern technology that allows traders to gather more consumer data, still protects the anonymity thereof, and whether the increased risk of identifying individual consumers, growing with each additional data collected by a trader, is accounted for by policymakers. Considering that the newly adopted data protection rules uphold the same level of protection, we may question their suitability to guarantee consumer privacy in the beginning era of the Internet of Things[12]. Paragraph three also illustrates what infringements of consumer privacy in (pre)contractual relationships could occur on the basis of collected data, through surveillance, targeted actions and profiling.

The right to privacy may become a victim of the fight for better consumer lifestyles, when policymakers and traders support the use of modern technology, without introducing a strict regulation thereof. Therefore, paragraphs four and five discuss two modern technological developments that, when applied to consumer contracts without the introduction of additional safeguards, may indeed weaken protection of consumer privacy. Modern technology allows retailers to label their products electronically using so-called RFID (Radio Frequency Identification) tags. That is to say, consumer products contain a smart chip that allows traders' to track them[13]. On the one hand, this technology allows traders to improve their stock management and theft prevention. On the other hand, these smart chips, if not deactivated upon purchase, may track consumers' behaviour[14]. The double-edged sword character of RFID tags is a known concern. In past years, the EU legislators commissioned data protection impact assessments to ensure sufficient consumer protection when traders use the RFID[15]. Paragraph four considers in more details the advantages and risks involved with allowing the use of RFID tags without strict oversight. The other example, presented in paragraph five, refers the issue of privacy to the purchase of consumer goods within the so-called 'Internet of Things', which to an extent also relies on the use of RFID tags[16]. For instance, when a consumer buys a smart fridge that can communicate with her oven, a smartphone and a car, she may not realize the impact these goods may have on her privacy. Paragraph five addresses the issue whether current data protection rules could still protect consumer's data and privacy in the new, 'smart' world.

The analysis of specific modern technologies gives an insight into the ongoing developments of consumer products and services, and allows predicting challenges that they will pose to the principle of consumer autonomy, as well as to the right to privacy. These challenges will be taken into consideration in the conclusions, while assessing whether policymakers could use these technologies

[10] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("Data Protection Directive") [1995] OJ L281/31.

[11] 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 ("ePrivacy Directive") [2002] OJ L201/37.

[12] Regulation 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 ("General Data Protection Regulation") [2016] OJ L119/89.

[13] See, in particular, Peslak (2005), pp. 327-328.

[14] Idem. See also: Eschet (2005), pp. 302-304.

[15] European Commission (2011) and European Commission (2014).

[16] See, in particular, Weber (2010), pp. 23-30.

either to support informed consumer choice or to influence market environment to the benefit of consumers.

2 Strategic policy objectives: healthy and sustainable consumption

According to the World Health Organization, worldwide obesity has more than doubled since 1980 and its main cause is the energy imbalance, i.e., consumption of more calories than their expenditure[17]. While promotion of healthy eating habits and lifestyles has long been on the policymakers' agenda, this growing undesirable trend raised questions as to how far policymakers could or should intervene to protect consumers from themselves. The European Commission funded research (the 'EATWELL' research project) to analyse the effectiveness of past diet and health related policy interventions, both on national and international level[18]. On the one hand, the EATWELL research project identified policy measures that support informed consumer choice, i.e., provide better information to consumers prior to their decision-making, in hope that informed consumers act rationally and make the 'right' contractual choice. On the other hand, in case informed choice strategies were not effective, the report also listed policy measures that could change the market environment. Through the use of these more intrusive policy measures, consumers would be more actively pushed towards making the 'right' choice[19].

Policymakers could thus try to influence consumer lifestyles either by ensuring that better information reaches consumers as to their options or they could obstruct, or even eliminate, some of consumer choices. The first type of strategy would call for policymakers to provide more consumer education and to improve, e.g., the readability of nutritional labels[20]. The second type requires policymakers to, e.g.: introduce higher taxes for undesirable food products; provide tax allowances and subsidies for healthy, nutritional food products[21]; introduce targets for certain harmful ingredients, like salt, in food products[22]. Modern technology could be useful in implementing either of these policies. Therefore, even though the report has not yet considered its advantages, we could expect policymakers to pay close attention to the technological developments and to be motivated to employ them, if research proves the effectiveness and efficiency of these measures in nudging consumers.

For example, the use of electronic, smart labels could potentially allow more information to reach consumers, in a more readable, standardized manner[23]. Smart labels would not have the space limitation of traditional labels, could encourage producers' creativity in conveying information to consumers, e.g., by allowing for the use of various graphs or colourful displays. Furthermore, electronic labels could facilitate a display of more personalized information, e.g., advising the consumer on the suitability of a given food product, considering consumer's blood sugar levels[24].

---

[17] See World Health Organization.
[18] See EATWELL (2013), p. 6.
[19] See EATWELL (2013), pp. 15-53.
[20] See EATWELL (2013), pp. 24-30.
[21] See EATWELL (2013), pp. 33-42.
[22] See EATWELL (2013), pp. 47-50.
[23] See, in particular, Sunstein (2012). On smart disclosure still failing to effectively inform consumers see, e.g., Kustin (2015).
[24] See, in particular, Kavis (2015).

It could also be beneficial for consumer health, if certain processed, harmful food products were taxed higher than healthy food products; if healthy food products were subsidized by the government to lower their prices; if producers of food products were challenged by the policymakers to lower the intake of such harmful substances, as salt. Also with regard to this second type of policies, modern technology could be useful in facilitating better control over the production, supply and distribution processes, as well as accounting for healthy food choices of consumers, and providing insights on how to nudge consumers to make such 'right' decisions. For instance, through RFID tags it could be easy to control the content of a 'smart' fridge and the consumer's intake of calories, salt, vitamins, etc. A far-going, intrusive measure would involve placing an automatic lockdown on a fridge, when consumers have reached the daily amounts that were set for them.

Similarly, policymakers could adopt the above-mentioned strategies in their quest to convince consumers to conclude more sustainable contracts. If we look at the textile industry, as an example, we may observe that producers of textile goods often have difficulties verifying the validity of corporate social responsibility ("CSR") claims and controlling the application of their CSR policies in the supply chain[25]. Also in this respect, intensifying the amount of awareness-raising campaigns may nudge consumers to consider CSR issues more often and may influence them when they are choosing between textile products of various brands, drawing their attention to fair trade brands. Additionally, policymakers may also steer consumer behaviour by adopting specific tax policy or setting specific targets for the textile industry. One of the most commonly mentioned benefits of using smart labels, as well as RFID tags, is their ability to tract the product throughout the supply chain, ensuring its visibility, and easy verification of any made CSR claims, which could ensure better enforcement of set targets[26].

It is clearly possible to use the new technology to the benefit of consumers, either by improving information provided to them, or by facilitating enforcement of consumer protection through the introduction of easy checkpoints of compliance with consumer policies. Policymakers could, therefore, consider prescribing the use of such technologies to traders, to an extent that this could help policymakers nudge consumers in making healthier and more sustainable contractual choices. However, this new technology could also be used to undermine consumer autonomy and to infringe consumer privacy, through surveillance, profiling and targeted action, as will be discussed in the following paragraphs. This potential of an abuse should, at least, give policymakers a pause in considering how to regulate the use of such technologies, and could discourage them from attempting to employ these technologies in their own strategies.

3 Chokepoint: the right to privacy & consumer autonomy

The right to privacy is a well-established constitutional right in most Member States, one of the fundamental rights of European citizens, protected under Article 8 of the European Convention on Human Rights[27]. This right to respect for private and family life, home and correspondence encompasses also a right to protection against the collection and use of personal data by the State

[25] See, in particular, European Commission (2013).
[26] See, in particular, Peslak (2005), p. 334.
[27] Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950, ETS 5, available at: <<http://www.refworld.org/docid/3ae6b3b04.html>>.

and its bodies[28]. In certain Member States national courts have also given this provision direct horizontal effect, allowing parties to invoke it in a private dispute[29]. However, even if this right would not be directly effective, consumers should be able to invoke it against a Member State, which introduced a policy leading to the infringement of their right to privacy. This could occur if, e.g., policymakers prescribed the use of certain technological means to traders, without introducing sufficient safeguards, which allowed for an invasive collection of consumers' personal data.

European consumers are additionally protected against undue collection and use of their data through the Data Protection Directive and ePrivacy Directive, recently updated by the new General Data Protection Regulation, which will start applying as of May 2018. Since modern technology increasingly facilitates traders' collection, storage and processing of consumers' data, it is progressively more difficult for policymakers to create a system of protection that would effectively block infringements of consumer privacy[30]. Especially, considering that policymakers are heavily lobbied by the business sector not to stand in the way of technological advances. Policymakers could, therefore, be inclined to leave it to the industry to decide how the modern technologies should guarantee consumer's personal data safety. Considering the feasible lack of standardization and low effectiveness of self-regulation in this respect, due to its non-binding effect[31], policymakers need to consider more carefully the impact of the lack of regulatory safeguards on consumers' constitutional and contract rights.

Many consumers, if aware of the occurrence of their data collection and processing, would likely consider their privacy invaded[32]. Conversely, consumers often seem rather at ease with 'selling' their privacy for various contractual benefits[33]. Some scholars suggest that this may signify the weakening of importance of the right to privacy as a fundamental right in modern times[34]. In case this assumption held, policymakers would not need to account for protection of privacy when considering their recommendations. However, I question this assumption, since consumer surveys seem to indicate consumers' lack of hope to be able to maintain their privacy in the face of advanced technological measures applied by traders and public authorities, rather than an alleviation of consumers' privacy concerns[35]. Alternatively, this could be seen as a an example of a systemic erosion of privacy by information technology that allowed for data to be collected at a mass scale, instantaneously, pervasively and often without consumer awareness thereof[36]. These online practices conflict with the status of the right to privacy as a fundamental right in Europe, but

[28] See, in particular, European Court of Human Rights (2016); ECHR, Copland vs The United Kingdom, judgment of 3 April 2007, No. 62617/00, para 42.
[29] See for the Netherlands, in particular, judgment of the Dutch Supreme Court of 9.01.1987 (*Edamse bijstandsmoeder*) NJ 1987/181.
[30] It took over four years of negotiations to adopt the new General Data Protection Regulation.
[31] See, in particular, Hildner (2006), pp. 146-148.
[32] See, in particular, Hildebrandt and Koops (2010), p. 436.
[33] See, in particular, De George (2002), pp. 269-270.
[34] See, in particular, De George (2002), p. 270, McArthur (2001), pp. 126-127 and Van Wel and Royakkers (2004), p. 136.
[35] 43% of European consumers worry that the information will be used without their knowledge, as well as that it will be shared with third parties without their consent, see, in particular, European Parliament (2011), p. 77.
[36] See, in particular, Hildebrandt and Koops (2010), p. 443.

enforcement thereof is neglected by the national regulators and authorities[37]. Despite inefficient enforcement, the right to privacy remains a fundamental right and we may expect policymakers to give proper consideration to the status and observance thereof, when drafting new rules[38].

Infringements of the consumers' constitutional right to privacy may affect the consumers' freedom of choice as to what contract to conclude, and on what terms, consequently eroding party autonomy, one of the main principles governing contract law[39]. If traders collect consumers' data and their preferences, they may use these to manipulate consumers into making choices in line with their, rather than with consumers', interests[40]. Currently, data protection laws in the EU aim at protecting consumers from such practices that would allow for the identification of a particular consumer on the basis of the collected data[41]. Any practices that would fully anonymise the data would be exempt from restrictions set by these laws[42]. Some scholars have argued that no data may be considered fully anonymised, that through connecting various anonymised data a specific consumer could be identified and this data used against her[43]. Still, policymakers allow generic aggregation of data to occur, through the use of anonymisation techniques, even if they are aware that these are imperfect, and that with a certain effort de-anonymisation could succeed[44]. Generally, modern technologies referred to in this chapter collect such aggregate, anonymised data, but the question remains how deep this anonymisation goes and how well do they protect personal data of consumers.

Various available modern technologies allow traders to collect a multitude of consumer data online. As a result, despite anonymisation of consumer data, traders have previously been able to, e.g., identify websites that women visit when they are expecting, or products they start purchasing at the beginning of their pregnancy. Consequently, consumers assigned to this group could receive targeted advertising recommending pregnancy supplements. Even if the name of a particular consumer is not revealed to traders, they obtain in this case personal data on consumer's health and know how to reach this consumer. The targeted advertising that is likely to follow may be in line with disclosed preferences of consumers, urging them to make already planned purchases in specific online shops[45]. This could be seen as a relatively minimally invasive measure. Alternatively, traders could try to change consumer preferences either by showing them advertisements for options they have not yet considered, or by enabling easier pursuit of some options over others, drawing more consumer attention to them. These targeted actions could not only hinder consumer autonomy by changing the market environment, but also infringe consumer privacy[46]. If policymakers prescribe the use of technologies that would allow for such practices to continue, we could wonder whether

[37] See, in particular, on the need to improve enforcement of the right to privacy through the adoption of the General Data Protection Regulation, European Commission (2015).
[38] European Commission (2016b), p. 10.
[39] See, in particular, Eidenmüller H (2009), pp. 116-117.
[40] See, in particular, Hildebrandt and Koops (2010), p. 436.
[41] See Recital 26 and Article 6 para 1 lit. 2 Data Protection Directive, as well as Recital 9, Articles 6 and 9 ePrivacy Directive.
[42] See for the continuation of this policy also Recital 26 of the General Data Protection Regulation.
[43] See, in particular, Malin B, Sweeney L, Newton E (2003).
[44] See, in particular, Article 29 Data Protection Working Party (2014).
[45] Or in some drastic cases even notifying consumers' families that they are pregnant, see, in particular, Hill (2012).
[46] It is, however, beyond the scope of this chapter to consider the scope of targeted actions that would lead to the infringement of consumer privacy and consumer autonomy.

they should be liable for any breach to consumer privacy that would result from the application of such technologies.

Aside targeted actions, the other infringement to consumer privacy and consumer autonomy through the use of modern technology could occur through profiling. Policymakers could potentially start cooperating with search engines such as Google and ensure that, whenever a consumer online is identified as a pregnant woman, search results popping up first on the consumer's screen would be related to healthy lifestyle choices for pregnant women. Since consumers are more likely to read only through first search results[47], they would be nudged towards making the 'choice' policymakers foresee for them. A combination of profiling and targeted action techniques could, therefore, lead to a change in the market environment. Moreover, such manipulation of search results may not only infringe consumer privacy, but also their right to equal treatment, as search engines could be set to not reveal certain options to consumers qualified by algorithms as, e.g., not being able to afford them or, contrarily, could show different prices for the same products or services to different consumers, varied accordingly to the data collected about a particular consumer[48].

Finally, surveillance is the most commonly considered breach of consumer privacy[49]. If the collected online data allows, with the use of resources, to identify a particular consumer, it is imaginable that she could be traced both in the online and offline environment. Through following consumer's steps, traders could gather more information on her and then use profiling and targeted actions to personalize information provided to this consumer, as well as, potentially, adjust the market environment surrounding this consumer to better meet her needs.

This paragraph elaborated further on the infringements to consumer privacy that could be likely to occur with the introduction of modern technologies. Policymakers should keep in mind the need to protect this fundamental right, when considering the need for adoption of a regulation applicable to such technologies, as well as, when using them to either influence consumer information or to change the market environment. The following paragraphs will look more closely into specific new technological developments that could be of service to policymakers in the pursuit of their goals, but at the same time may endanger the protection of consumer privacy.

4 Trojan horse: RFID

The European legislators are currently considering further regulation of the RFID, which could even require mandatory application thereof by producers of textile products[50]. This is under consideration, as RFID's assets in the enforcement of CSR policies seem plentiful. With a little investment, it could assist producers and suppliers in achieving better control over the production and supply chain, which could lower production costs, and, therefore, also cut consumer prices[51]. Moreover, it could confirm producers' CSR claims, providing consumers with an insight into the sustainability of the production and supply chain of the textile industry. Therefore, it seems unquestionable that the RFID's use could increase contractual efficiency and, as such, could also be of interest to policymakers. Additionally, some of its features that are further discussed in this

[47] 75% of internet users never read past the first page of search results, see, in particular, Slu (2012).
[48] See, in particular, Hildebrandt and Koops (2010), p. 437.
[49] See further on this in the following paragraph.
[50] See fn 15.
[51] See, in particular, Weiss (2003), p. 25.

paragraph could enable policymakers to nudge consumers to make specific choices. Unfortunately, so far, reports on the functioning and the security of the RFID technology show that it does not sufficiently guarantee consumer privacy[52]. Indeed, if policymakers are tempted to prescribe its use, they may cause significant damage to this fundamental right and its enforcement.

The use of the RFID, even though spreading, often remains a mystery to consumers, who either may be unaware of its operation or of a risk it may pose to their privacy[53]. There is currently no legal obligation for products with an embedded RFID tag to communicate this on the packaging or on a label. Furthermore, an addition of an RFID tag may not signify to consumers that their data could be collected and processed through this chip. They may trust in the assurances of traders and producers of products with RFID tags that they only use these tags to improve their inventory management, or the supply chain, etc. However, privacy advocates notice that currently no guarantees can be made or are being made that traders will switch these chips off at the moment of consumer purchase. This means that consumers purchasing a pair of trousers labelled with an RFID tag, showing, e.g., that these pants were made in fair trade conditions, could potentially be followed home, through the use of the same chip[54]. Since RFID tags do not require a direct line of sight to be read, unlike barcodes, the data stored on them could be collected by an RFID reader nearby the product. Obviously, in order to systematically track the consumer's location a whole infrastructure of RFID readers would need to be installed and operated, but random checkpoints could suffice to collect some personal data of a given consumer[55]. This could occur without consumers ever consenting to their data being collected and processed, and even with them remaining unaware that such a practice occurs[56]. RFID tags could, therefore, quite easily be used for surveillance and, as such, endanger protection of consumer privacy.

Unfortunately, surveillance is just one of the potential privacy infringements that could materialize through the use of RFID tags. As mentioned in the previous paragraph, traders could also use it for profiling and targeted actions[57]. For instance, a reader of RFID tags installed in a warehouse could identify products already placed in a consumer's shopping cart and show her, when she is moving throughout the store, personalized, virtual advertisements of products that the database would estimate could be of interest for this particular consumer[58].

We may distinguish the risk associated with the use of the RFID from general consumer fears of privacy infringements, since information collected through RFID tags would be in the hands of private parties, traders, and not of publicly regulated bodies[59]. Already the use of cookies by online traders and advertisers caused a lot of consumer concerns, and raised issues of potential privacy

[52] Idem; See also Peslak (2005), pp. 333-334.
[53] See, in particular, Eschet (2005), p. 311 and Hildner (2006), p. 160.
[54] See, in particular, Weiss (2003), p. 28. For example, in Texas RFID tags are used to track the movement of school children, creating a record of them entering and exiting school buses and providing an early warning system in case of a kidnapping, see: Richtel (2004), pp. 1-3.
[55] See, in particular, Weiss (2003), p. 29.
[56] See, in particular, Hildner (2006), p. 140.
[57] See, in particular, Hildner (2006), p. 141.
[58] See on similar practices through the use of eye-tracking technology in: Lewinski, Trzaskowski and Luzak, (2016).
[59] See, in particular, Hildner (2006), p. 139.

infringements[60], but the RFID has a potential to become more invasive, as it would track consumers also offline. For these reasons, privacy advocates suggest that the industry should introduce certain safeguards whenever they use RFID tags.

One such security measure is a 'kill switch' that could be installed on all RFID tags. Through the use of this switch, it would be possible to disable RFID tags at the moment of consumer's purchase, or, at the latest, when consumers leave the store with the product[61]. Policymakers could, therefore, consider regulating only such RFID tags that would become passive with the consumer's purchase of the goods and prohibiting the use of the RFID without these safeguards. This may, however, not be that easy to either apply in practice or to enforce. Moreover, policymakers have already had experience with the issues of privacy by design. For the privacy protection to be effective, policymakers would need to categorically prohibit the use of RFID tags outside the production, supply and distribution chain, regardless of the consumer's choice in this respect. That is to say, traders could not expect consumers to 'opt-out' from the RFID tag's activity, whether it would be by asking consumers to activate this switch, or through the consumer's notification duty that the trader should disable the tag.

Another option leaves the choice entirely to consumers whether to deactivate the RFID tag by providing them with so-called blocker tags[62]. There are various ways, in which this technology could operate, but generally it would be at the consumers' discretion to switch the RFID tag on and off. This solution could be beneficial to consumers if the RFID tag would provide them with some information that could be useful also in post-contractual situations, and they had an option to access it through their own readers. However, it also brings with it the risk of consumers forgetting to deactivate the RFID tag after the use. Not to mention, either policymakers through regulation or traders in practice would decide on the default setting for the RFID tag. That is to say, whether consumers would leave the store with a product with an embedded RFID tag switched on or off. Due to various consumer biases that may discourage consumers from changing the status quo[63], in order to better protect consumer privacy this solution should come with a default passive setting for the RFID tag.

Traders have an incentive to implement RFID tags, since these could increase the efficiency of their production and supply chain[64]. Considering the above-mentioned risks to privacy protection, the question arises whether the objectives of policymakers to encourage healthy and sustainable lifestyles compensate the risk involved, if they were to recommend the RFID's use to traders.

The benefits of the use of RFID tags for policymakers could be manifold. For instance, through the use of RFID traders could simplify product labelling and thus, likely, better support informed consumer choice. They could place auxiliary information on the RFID tags instead of on the product's

[60] See, in particular, Luzak (2013), pp. 221–245.
[61] See, in particular, Privacy Rights Clearinghouse (2003) and Hildner (2006), p. 148.
[62] See, in particular, Juels, Rivest, Szydlo (2003), pp. 103-111 and Hildner (2006), pp. 147-148.
[63] See, in particular, Baron and Ritov (1994), pp. 478-479, Schweitzer (1994), p. 459 and Gilovich, Husted Medvec and Chen (1995), p. 189.
[64] Although, even traders are concerned about consumer perception of the RFID tags. For example, shortly upon announcing a trial use of 'smart shelves', on which RFID-tagged Gillette razors would be displayed, Wal-Mart withdrew its campaign. The official reason was a change to its operational strategy, but it seems clear that the change in strategy was motivated by privacy concerns. See e.g. Weiss (2003), pp. 27-28.

label, which could benefit consumer understanding of labels by limiting the amount of directly disclosed information. Simultaneously, through the RFID tags traders could give consumers an access to more information than a traditional label would allow for, due to its size limitations. This information could also be made more visible, since there would not be a need to limit the font's size, and attractive, through the use of, e.g., colourful graphs and diagrams[65]. This means that if only consumers were aware of the RFID tag and how to use it, had access to RFID tags' readers, they could potentially be better informed on nutrition, CSR-related claims, etc. It would require empirical research to assess whether consumers would make an effort to access the information stored on the chip, since currently they seem to be mostly passive in their reception of contractual information[66]. Further research could also inquire whether traders would indeed be inclined to optimize the readability of information on the RFID tags and whether it would be easier to comprehend for consumers, as well as, whether placing auxiliary information thereon instead of on the label would improve readership, and understanding of labels. Conditional on the outcome of this research, policymakers could consider recommending the use of RFID tags to traders, and addressing privacy concerns related thereto, if through the use of the RFID consumers would be better informed, and, as a result, they would be more likely to make healthier and more sustainable choices.

Alternatively, RFID tags could be used to change the market environment or, at least, to ensure the suitability of the market environment. The RFID enables tracking the product through the distribution process, allowing both traders and consumers to confirm whether this product was produced in a sustainable, fair trade manner. This would facilitate policymakers in their enforcement of consumer protection against misleading commercial practices, as well as, ensure that there is no confusion among consumers, which contractual choices are contributing to sustainable environment. If the policymakers would recognize the use of RFID tags as a method to promote better consumer lifestyles, they would, however, need to carefully consider what rules would need to be adopted to protect individual consumers' interests and how these could be enforced.

To further analyse potential benefits of the use of RFID tags, it is important to consider their role in the Internet of Things, which follows in the next paragraph.

5 Divide and conquer: Internet of Things

The Internet of Things describes a world, in which advanced technology allows various machines and computers to communicate with each other, allowing people to connect and interact with the digital environment[67]. The data communicated between the machines often concerns consumers, their lifestyles and various behaviour, which could enable these machines to personalize services to a given consumer. Consequently, in order for the Internet of Things to function properly, both technology and legal provisions need to allow machines to collect and process consumers' personal data, enabling them to establish consumer identity, even if it was just their virtual identity[68]. As a result of the data exchange between the machines, consumers could expect that their needs would be easier and better met by their environment.

[65] For instance, in a Prada store in NYC changing rooms track RFID tags on a selected by the consumer product and show her accessories that go with it, see Hildner (2006), p. 136.
[66] See, in particular, Luzak (2015), pp. 79-87 and Milne and Culnan (2004), pp. 17, 19, 23-25.
[67] See, in particular, Sarma and Girão (2009), p. 359.
[68] Idem.

For instance, consumers going for a run while wearing a smartwatch that measures their speed, their heart rhythm and the amount of burned calories, could expect this smartwatch to communicate to the fridge how many calories they have burned during this activity. The fridge, having received this communication, could message the consumer's smartphone with the list of groceries necessary to replenish these calories, considering what products may be missing from it, as well as the consumer's food preferences. Possibly, the fridge would receive a message from a computer in the doctor's office, which the consumer visits, confirming products the consumer is allergic to or should avoid for dietary concerns, which would influence the grocery list, as well. The improvement of the control over consumer health data is definitely one expected beneficial effect of the Internet of Things[69]. Such improved communication between various machines would not only allow to better inform consumers, but would also lead to the creation of a different market environment, in the above-mentioned example in the health sector, specifically.

Another advantage of the Internet of Things would be providing consumers with more control over the environment they inhabit. The most commonly used example in the literature concerns energy savings. We may imagine a consumer's computer screen communicating with the computer, ensuring automatic switch off of the screen, if the consumer forgot about this when shutting down the computer. Lights, heating and air-conditioning in the consumer's apartment could all be notified by the consumer's car or a smartphone about the consumer's time of arrival, and turn on at the appropriate, convenient for the consumer time[70]. With regard to the above-used example of the textile industry, we could again imagine a consumer's smartphone communicating with the consumer's digitalized wardrobe, informing consumer whether a certain T-shirt she spotted in the store would match with the skirt in her wardrobe. Again, more personalized and detailed information could facilitate consumers in making better contractual decisions.

The above-mentioned examples illustrate just some, selected aspects of further developing the Internet of Things. Consumers may very well be attracted to the futuristic lifestyle, but the use of the Internet of Things holds a lot of potential also for traders and policymakers. Having a better insight into the supply chain, shop managers could have more control over the stocked products, which could, e.g., curb the waste of food products and contribute to more sustainable economy[71]. More real-time information on the transportation of goods would allow freight companies to optimize their deliveries and lead to additional energy savings[72]. Policymakers could optimize healthcare, e.g.: by using better health sensors they could easier identify patients with allergies; by introducing automatic adjusting of doses of prescribed medications, according to patients' health stats, without the need for in-person doctor or nurse consultations[73]. The Internet of Things could, therefore, easily allow changing the market environment. Policymakers should be interested in retaining some control over this process, since they could use these technologies themselves to increase their influence over consumers and their decision-making. Also in this case, however, policymakers should conduct a careful check of potential benefits and risks involved with the further-reaching introduction of the Internet of Things.

[69] See, in particular, Atzori, Iera and Morabito (2010), p. 2794.
[70] Idem, p. 2795.
[71] See, in particular, Atzori, Iera and Morabito (2010), p. 2794.
[72] Idem.
[73] Idem, p. 2795.

Many consumers will perceive the above-described Internet of Things as what they always imagined XXI century to look like, having watched movies like 'The Fifth Element', 'The Terminator' or even 'Avatar', but they should also keep in mind 'Minority Report' and 'The Matrix', clearly illustrating additional privacy concerns. The Internet of Things is a broad term that may apply to any combination of goods and services, which facilitate the above-mentioned communication between the machines. Some of the machines would be able to interface with others due to a presence of an RFID tag, but other technologies are likely to be employed, as well[74]. Regardless of the particular technology used, the machines' objective is to collect consumer data and share it with other machines. We may, therefore, clearly identify a risk to consumer privacy involved with the use of the Internet of Things.

With various machines being able to collect consumer data, there is a need to ensure that these machines observe privacy policies individually, but also together, when the data is aggregated. Unfortunately, through the introduction of various points of data collection, remaining possibly under control of different market players, with no specified rules that apply in this situation, it is hard to foresee, how consumer data could be held secured. Many questions arise in connection to the possible division of responsibility for privacy protection between producers or data controllers of different components of the Internet of Things.

The first inquiry could be, as to whether within the Internet of Things one machine should be identified as the core centre of data collection and exchange, which could make its producer a data controller, responsible for ensuring privacy protection of all data flowing between the interconnected machines. Alternative strategy would be to continue to hold responsible for privacy protection only this data controller who has collected, processed and then shared consumer data, within his part of the Internet of Things network. In this last case scenario, since the purpose of the Internet of Things is to facilitate data flow between various machines, we need to ask who then bears this burden during the transmission of data between the machines. Moreover, if the responsibility for privacy protection is shared, it may be difficult to establish at what moment that responsibility passes from one data controller to another, considering constant data flow. To look at it practically, we may ask whether a producer of a smart fridge could be able to control privacy protection settings on a smartphone that the fridge is communicating with. The Internet of Things not only enables data flow between the machines, but also may infer some conclusions from the aggregated data. Who would bear the responsibility for the data that was aggregated from individual inputs, that is to say, collected separately by each machine?

Since the Internet of Things would require an involvement of complex technology, we may foresee that consumers would not be familiar with its functioning and processes, which could also leave them unaware of potential privacy infringements. Policymakers should consider introducing information duties about data collection through the machines of the Internet of Things, letting consumers know when, by whom and for what purposes their data is gathered. Ideally, consumers would also be granted some control over this process, but up-to-date experiences with online privacy protection do not leave much optimism that this could be achieved; with traders setting the

[74] See, in particular, Atzori, Iera and Morabito (2010), pp. 2787-2789 and Weber (2010), p. 23. Technologies are constantly developing, but we could expect Near Field Communications (NFC) and Wireless Sensor and Actuator Networks (WSAN) to work together with RFID tags.

defaults in a way granting them consumers' consent to the collection and the use of their data, or restricting access to online content, if consumers do not provide their consent[75].

Again, the potential for breach of privacy protection seems to outweigh the benefits of facilitating more healthy and sustainable consumer lives. However, the European legislators remain optimistic that proper regulation could be found and with it, the investment in further development of the Internet of Things could yield good results. Currently, there are no specific rules applying to the Internet of Things. The European Commission started to place more emphasis on the regulation of the digital single market, but the so-far proposed regulations do not venture into the area of the Internet of Things, except for encouraging better interoperability between consumer technologies[76]. There are, however, ongoing research projects and collaboration of the European legislators and relevant stakeholders into the possibility of further development of the Internet of Things, and its regulation.

For instance, in March 2015 the European Commission created the Alliance for Internet of Things Innovation ("AIOTI"), within which it aims to closely cooperate with relevant stakeholders, encouraging further technological developments and standardisation policies[77]. This follows earlier adoption of non-binding measures, in which attention was mostly given to the consumers' need to be able to disconnect from the digital environment at any time, and to be able to disable the RFID tags[78]. In 2016 the European Commission published also a staff working document on how to advance the Internet of Things in Europe[79]. One of the risks mentioned in this document concerns the risk of the Internet of Things developing independently of the already established principles of data protection, privacy and security, which could force consumers to share their data against their will. The European legislator, therefore, makes it clear that any further development in this sector would need to comply with the fundamental rights, such as the right to privacy and data protection[80]. However, no specific measures have until now been adopted or even agreed on.

6 Conclusions

This chapter's analysis of the impact that the modern technology may have on consumer lifestyles and their privacy, clearly shows a great potential of these new measures, not only when traders use them, but also, as to what policymakers could achieve, if they employed them. The fight against unhealthy and unsustainable consumer lifestyles has so far not showed major breakthroughs. Consumers remain uninformed or unmotivated to change their habits, or underestimate the risks involved with continuing on their merry, but destructive life paths. New, more efficient and effective tools for nudging consumers to making the 'right' contractual choices could tip the scales, bringing policymakers closer to reaching their objectives.

From this perspective, policymakers may consider using the modern technology either for improving consumer information or to influence the market environment. In the first case, the level of invasiveness into consumer lifestyles and their privacy is lower, since policymakers would still leave

[75] See, for instance, Luzak (2013), pp. 221-245.
[76] See, in particular, European Commission (2016a).
[77] See Van Der Klauw (2016).
[78] See, in particular, European Commission (2009).
[79] European Commission (2016b).
[80] Idem, p. 10.

the contractual choice to the consumer to make, and only facilitate informed decision-making. In the second scenario, policymakers would be more active in nudging consumers, likely hiding certain, considered less healthy and less sustainable, contractual options from them and pushing them onto the socially-desired path. The choice between these measures would, therefore, likely make a difference as to whether consumers could keep their contractual autonomy. In either case, however, to employ these measures, policymakers and traders would first need to gather extensive information on the consumer and her preferences, endangering consumer privacy.

Each war has its victims and it is feasible that the protection of the right to privacy and the principle of consumer autonomy could be the victim of the fight against unhealthy and unsustainable lifestyles. So far, the European legislator does not seem to be ready to dispose privacy and data protection of their status as fundamental rights[81]. However, protection of privacy is not mentioned as the first or even one of the most major concerns, when the European Commission considers further development of the Internet of Things. Instead, technological and financial issues related to this progress seem to be the frontrunners on the list of issues that need to be tackled prior to the implementation of the Internet of Things. This may not bode well for the future of the right to privacy. This data suggests that the answer to the research question posed in this chapter is that the policymakers only marginally, if at all, consider the need for protection of consumer privacy when regulating the use of modern technology, and this answer would likely not change when it concerned the use of this technology to nudge consumers towards healthy and sustainable contracts.

Since modern technologies are constantly developing, policymakers should keep a close vigil over them and not be afraid to introduce rules that would ensure consumer data safety and security. In any case, policymakers should conduct a careful check of benefits and risks involved and continue to invest in research, gathering of empirical evidence on the functioning, and the impact of these modern technologies on contractual and constitutional principles and rights.

[81] Idem.

References

Alemanno A, Sibony A-L (2015) Nudge and the Law: A European Perspective. Hart Publishing, Oxford

Article 29 Data Protection Working Party (2014) Opinion 05/2014 on Anonymisation Techniques. 10 Apr 2014, 0829/14/EN/WP216. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Accessed 30 Jun 2016

Atzori L, Iera A, Morabito G (2010) The Internet of Things: A survey. Computer Networks 54:2787-2805

Baron J, Ritov I (1994) Reference Points and Omission Bias. Organizational Behavior and Human Decision Processes 59:475-498

Boseley S (2014) UK among worst in western Europe for level of overweight and obese people. In: The Guardian 29, May 2014. https://www.theguardian.com/society/2014/may/29/uk-western-europe-obesity-study. Accessed 30 Jun 2016

Carolan E, Spina A (2015) Behavioural Science and EU Data Protection Law: Challenges and Opportunities. In: Alemanno A, Sibony A-L (eds.) Nudge and the Law: A European Perspective. Hart Publishing, Oxford, p 161-178

Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5, available at: http://www.refworld.org/docid/3ae6b3b04.html. Accessed 30 Jun 2016

Danyliak A (2015) Who's a real fashion victim?. In: European Year for Development, 11 Dec 2015. https://europa.eu/eyd2015/en/international-young-naturefriends/posts/fashion-and-sustainability. Accessed 30 Jun 2016

De George RT (2002) Business Ethics and the Information Age. Business and Society Review 104:261-278

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31

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

Dutch Supreme Court judgment of 9.01.1987 (*Edamse bijstandsmoeder*) NJ 1987/181

EATWELL (2013) Effectiveness of Policy interventions to Promote Healthy Eating and Recommendations for Future Action: Evidence from the EATWELL Project. http://eatwellproject.eu/en/upload/Reports/Deliverable%205_1.pdf. Accessed 30 Jun 2016

ECHR, Copland vs The United Kingdom, judgment of 3 April 2007, No. 62617/00

EHLA (European Healthy Lifestyle Alliance). http://www.ehla-europe.eu/risk-factors-and-prevention/. Accessed 30 Jun 2016

Eidenmüller H (2009) Party Autonomy, Distributive Justice and the Conclusion of Contracts in the DCFR. European Review of Contract Law 5:109-131

Eschet G (2005) FIPs and PETs for RFID: Protecting Privacy in the Web of Radio Frequency Identification. Jurimetrics 45:301-332

European Commission (2009) Internet of Things – An action plan for Europe. In: Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions, COM(2009) 278 final, 18 Jun 2009. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0278:FIN:EN:PDF. Accessed 30 Jun 2016

European Commission (2011) The Privacy and Data Protection Impact Assessment Framework for RFID Applications: A defining moment in the modern epic of co-regulation in ICT. In: Digital Single Market blog, 8 Apr 2011. https://ec.europa.eu/digital-single-market/en/blog/the-privacy-and-data-protection-impact-assessment-framework-for-rfid-applications-a-defining-moment-in-the-modern-epic-of-co-regulation-in-ict. Accessed 30 Jun 2016

European Commission (2013) Sustainability of textiles. In: Retail Forum for Sustainability Issue Paper No 11, Aug 2013. http://ec.europa.eu/environment/industry/retail/pdf/issue_paper_textiles.pdf. Accessed 30 Jun 2016

European Commission (2014) Digital privacy: EU-wide logo and “data protection impact assessments” aim to boost the use of RFID systems. In: Press release, 30 Jul 2014. http://europa.eu/rapid/press-release_IP-14-889_en.htm. Accessed 30 Jun 2016

European Commission (2015) Questions and Answers – Data protection reform. In: Press release, 21 Dec 2015. http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm. Accessed 30 Jun 2016

European Commission (2016a) Commission proposes new e-commerce rules to help consumers and companies reap full benefit of Single Market. In: Press release, 25 May 2016. http://europa.eu/rapid/press-release_IP-16-1887_en.htm. Accessed 30 Jun 2016

European Commission (2016b) Advancing the Internet of Things in Europe. In: Commission Staff Working Document SWD(2016) 110/2. https://ec.europa.eu/digital-single-market/en/news/staff-working-document-advancing-internet-things-europe. Accessed 30 Jun 2016

European Commission. Overweight and obesity – BMI statistics. In: Eurostat. http://ec.europa.eu/eurostat/statistics-explained/index.php/Overweight_and_obesity_-_BMI_statistics. Accessed 30 Jun 2016

European Court of Human Rights (2016) Personal Data Protection. In: Documents, Apr 2016. http://www.echr.coe.int/Documents/FS_Data_ENG.pdf. Accessed 30 Jun 2016

European Parliament (2011) Consumer behaviour in a digital environment. Study. In: IMCO (Committee on the Internal Market and Consumer Protection of the European Parliament), Aug 2011,

http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=42591. Accessed 30 Jun 2016

European Parliament (2014) Workers' conditions in the textile and clothing sector: just an Asian affair? Issues at stake after the Rana Plaza tragedy. In: European Parliament Briefing, Aug 2014. http://www.europarl.europa.eu/EPRS/140841REV1-Workers-conditions-in-the-textile-and-clothing-sector-just-an-Asian-affair-FINAL.pdf. Accessed 30 Jun 2016

Gilovich T, Husted Medvec V, Chen S (1995) Commission, Omission and Dissonance Reduction: Coping with Regret in the "Monty Hall" Problem. Personality and Social Psychology Bulletin 21:182-190

Hildebrandt M, Koops B-J (2010) The Challenges of Ambient Law and Legal Protection in the Profiling Era. The Modern Law Review 73:428-460

Hildner L (2006) Defusing the Threat of RFID: Protecting Consumer Privacy Through Technology-Specific Legislation at the State Level. Harvard Civil Rights-Civil Liberties Law Review 41:133-176

Hill K (2012) How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did. In: Forbes, 16 Feb 2012. http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#7f5fdc6234c6. Accessed 30 Jun 2016

Juels A, Rivest RL, Szydlo M (2003) The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. Proceedings of the 10th ACM conference on Computer and communications security. http://dl.acm.org/citation.cfm?id=948126. Accessed 30 Jun 2016

Kavis M (2015) The Smart Labels That Will Power The Internet of Things. In: Forbes, 17 Feb 2015. http://www.forbes.com/sites/mikekavis/2015/02/17/the-smart-labels-that-will-power-the-internet-of-things/2/#4cc19fcc75e8. Accessed 30 Jun 2016

Knapton S (2016) British people will be fattest in Europe by 2025. In: Telegraph, 31 Mar 2016. http://www.telegraph.co.uk/science/2016/03/31/british-people-will-be-fattest-in-europe-by-2025/. Accessed 30 Jun 2016

Kustin ME (2015) 10 Reasons Why GMO Smart Label Isn't 'Smart' at All. In: EcoWatch, 16 Dec 2015. http://ecowatch.com/2015/12/16/gmo-smart-label/. Accessed 30 Jun 2016

Lewinski P, Trzaskowski J, Luzak J (2016) Face and Emotion Recognition on Commercial Property under EU Data Protection Law. Psychology & Marketing (in press)

Luzak J (2013) Much Ado about Cookies: The European Debate on the New Provisions of the ePrivacy Directive regarding Cookies. European Review of Private Law 21:221–245

Luzak J (2015) Online disclosure rules of the Consumer Rights Directive: Protecting passive or active consumers?. Journal of European Consumer and Market Law 3:79-87.

Malin B, Sweeney L, Newton E (2003) Trail re-identification: learning who you are from where you have been. In: Carnegie Mellon University, Mar 2003. http://dataprivacylab.org/dataprivacy/projects/trails/paper3.pdf. Accessed 30 Jun 2016

McArthur RL (2001) Reasonable expectations of privacy. Ethics and Information Technology 3:123-128

Milne GR, Culnan MJ (2004) Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices. Journal of Interactive Marketing 18:15-29.

Niemtzow E (2013) Are consumers done with fast fashion. In: BSR blog, 4 Jun 2013. http://www.bsr.org/en/our-insights/blog-view/are-consumers-done-with-fast-fashion. Accessed 30 Jun 2016

Oliver A, Ubel P (2014) Nudging the obese: a UK-US consideration. Health Economics, Policy and Law 9:329-342

Peslak AR (2005) An Ethical Exploration of Privacy and Radio Frequency Identification. Journal of Business Ethics 59:327-345

Privacy Rights Clearinghouse (2003) RFID Position Statement of Consumer Privacy and Civil Liberties Organizations. 20 Nov 2003. https://www.privacyrights.org/ar/RFIDposition.htm. Accessed 30 Jun 2016

Regulation 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 [2016] OJ L119/89

Richtel M (2004) In Texas, 28,000 Students Test an Electronic Eye. The New York Times, 17 Nov 2004

Sarma AC, Girão J (2009) Identities in the Future Internet of Things. Wireless Personal Communications 49:353-363

Schweitzer M (1994) Disentangling Status Quo and Omission Effects: An Experimental Analysis. Organizational Behavior and Human Decision Processes 58:457-476

Slu E (2012) 24 Eye-Popping SEO Statistics. In: Search Engine Journal, 19 Apr 2012. https://www.searchenginejournal.com/24-eye-popping-seo-statistics/42665/. Accessed 30 Jun 2016

Sunstein C (2012) Informing Consumers through Smart Disclosure. In: The White House blog, 30 Mar 2012. https://www.whitehouse.gov/blog/2012/03/30/informing-consumers-through-smart-disclosure. Accessed 30 Jun 2016

Van Der Klauw K (2016) Why there is more to the Internet of Things than just technology – the role of AIOTI. In: European Commission's Digital Single Market blog, 29 Jan 2016. https://ec.europa.eu/digital-single-market/en/blog/why-there-more-internet-things-just-technology-role-aioti. Accessed 30 Jun 2016

Van Wel L, Royakkers L (2004) Ethical issues in web data mining. Ethics and Information Technology 6:129-140

Waldron J (2014) It's All for Your Own Good. In: The New York Review of Books, 9 Oct 2014. http://www.nybooks.com/articles/2014/10/09/cass-sunstein-its-all-your-own-good/. Accessed 30 Jun 2016.

Weber RH (2010) Internet of Things – New security and privacy challenges. Computer Law & Security Review 26:23-30

Weiss A (2003) Me and My Shadow. netWorker 7:24-30

World Health Organization. http://www.who.int/mediacentre/factsheets/fs311/en/. Accessed 30 Jun 2016