WIK-Consult • Report

Study for Ofcom

Personal Data and Privacy

Final Report

Authors:
Dr René Arnold
Annette Hillebrand
Dr Martin Waldburger

WIK-Consult GmbH
Rhöndorfer Str. 68
53604 Bad Honnef
Germany

Bad Honnef, 26 May 2015

wik CONSULT

Contents

Executive summary **1**

Abbreviations **8**

1 Introduction **9**

2 The role of informed consent in privacy law **12**

2.1 Fundamental rights and general data protection law 12

2.2 Informed consent in the e-Privacy Directive 15

2.3 Future developments 18

3 The role of informed consent in practice **20**

3.1 Do consumers read? 20

3.2 Do consumers understand? 25

3.3 Do consumers act after reading? 32

4 Potential to improve informed consent in practice **39**

4.1 How to improve readership? 39

4.2 How to improve understanding? 42

4.3 How to improve the chance that consumers act upon information? 50

4.4 Informed consent could be improved by learning from a domain that made it work 54

5 Conclusions and possible future research **60**

6 Annex: Internet of Things and personal data **64**

7 Annex: Methodology **70**

8 Annex: Studies **71**

References **183**

Glossary **193**

Acknowledgements

The authors of the present report would like to express their gratitude to Prof Dr Natali Helberger and Dr Frederik J. Zuiderveen Borgesius from the University of Amsterdam for their valuable input and constructive comments towards the content of our report. In particular, we would like to point out that the work already conducted by Dr Frederik J. Zuiderveen Borgesius as part of his PhD thesis (in press) and his papers published from this work have helped the authors immensely to gain a broad overview of the research in this field as well as to structure the present report.

Furthermore, the authors would like to express their gratitude to Dr Aleecia M. McDonald (University of Stanford) for her constructive comments on the present report and to Dr Frederik J. Zuiderveen Borgesius for writing chapter 2..

Executive summary

Numerous online services provide useful information and content to consumers, often with the aid of personal data. We observe the emergence and wide-spread use of innovative services where sharing personal data results in visible benefits to consumers. We likewise observe data to become an increasingly important input to the successful implementation of business models in the data-driven economy. The increased use of data-driven services made clear that new opportunities and challenges to personal data and privacy arise. Most importantly, the role informed consent plays for and in online services deserves close examination.

In this context, this report provides a literature review conducted on behalf of Ofcom on personal data and privacy. The study sought to understand (1) the role of informed consent in privacy law, (2) the role of informed consent in practice and (3) potential ways to improve informed consent in practice. Furthermore, the study investigated the impact of the Internet of Things on the three major issues. The executive summary is also structured around these three major issues.

The role of informed consent in privacy law

From a legal point of view, the stance on personal data and privacy is clear-cut. The right to protection of personal data is a fundamental right constituted in the European Union, and the European Data Protection Directive of 1995 which is implemented by the member states. The directive entails specific requirements for the processing of personal data. Within that, informed consent plays a central role. With respect to online marketing practices, it is important to realise that in Europe informed consent is needed both for placing cookies or similar tracking devices on user's computers, according to the e-Privacy Directive, as well as for ensuing collection and processing of personal data, as regulated by the Data Protection Directive. There are instances in which consent is not required, e.g. if a cookie is necessary for transmission of communication, or for a service explicitly requested by the user. Furthermore, many personal data processing activities can be based on another legal basis than the data subject's consent. For instance, if the fulfilment of the specific service requires processing of personal data, consent is not always required. Nevertheless, consent plays a central role in the rules for online data processing.

The role of informed consent in practice

Consumers rarely read terms and conditions at all.

The signing-without-reading problem or, in the online environment, the clicking-without-reading problem is a well-documented phenomenon. Consumers agree to terms and conditions in all sorts of situations that may or may not have an impact on who can access their personal data, analyse it and potentially use it for action that consumers

may feel uncomfortable about. In fact, consumer surveys consistently show that consumers do say they worry about their personal data and what happens with it. However, in practice, they show very little if any interest in engaging with terms and conditions or even more specifically privacy policies. The most seminal study in this area finds that only about 0.05% of agreements are actually accessed by consumers before they consent to them. It was found that access does not necessarily translate into consumers actually having read the terms and conditions as the average time spent viewing the content of the agreements was significantly below one minute. Understandably, this is not enough to grasp the meaning of the respective agreement.

Time is also the reason commonly identified in the literature for why consumers do not engage in reading terms and conditions. As these texts are usually difficult and cumbersome to read, consumers rarely bother. In fact, if one were to read all the terms and conditions of the websites one visits throughout a year, this would take up several weeks assuming a full 40 hours of reading time each week. Given that the vast majority of website visits last no longer than 15 seconds, consumers' low rate of engagement is not surprising although it does contradict how strongly consumers usually say they feel about protecting their personal data, which is reported in various surveys. This contradiction is commonly referred to as the "privacy paradox".

Here, it should be noted that the online environment facilitates the clicking-without-reading phenomenon compared to the offline signing-without-reading phenomenon to some extent. For instance, there is no one there to point the consumer to the important parts of the terms and conditions. There is also no physical signature involved, which may present a stronger barrier than a simple click of a button. In fact, setting the default option to "agree" may further facilitate consumers' signing-without-reading for online privacy policies as humans have a tendency to stick to the default option. Furthermore, consumers are strikingly unaware of what happens with their personal data. For instance, they are commonly surprised to learn that their browsing history is analysed and used for targeted advertising. So, they may also believe that there is no harm in not reading privacy policies. Finally, browse-wrap contracts (i.e. agreeing to terms simply by using a website) may even impede the consumer from becoming aware of agreeing to a contract completely.

If they read them, they usually have difficulty understanding them.

Commonly, the length of terms and conditions and the legalistic jargon are blamed for consumers not being able to understand them. In fact, even law students were found to have significant problems understanding them. Studies investigating the readability of terms and conditions consistently find that at least university-level reading skills are needed to understand them.

However, as the reviewed literature indicates, the problem may start even at an earlier stage. Several studies highlight that consumers already have great difficulty

understanding the term “privacy policy” as it misleads them to believe that there is a policy in place to protect their privacy. Thus, it is not surprising that the mere presence of a privacy policy inclines consumers to disclose more personal information. Privacy labels or seals or other graphical representations are likely to increase this effect, in particular when one’s involvement with privacy issues is low.

It is equally difficult if not impossible for consumers to understand the consequences with respect to personal data processing. This is due to information asymmetry, which is substantially fostered by the complexity of the continuously evolving system of data flows mediated by data aggregators, ad networks, ad exchanges and third-party tracking companies.

Consumers cannot evade online tracking, but they cope with the effects.

Consistently, the literature indicates that consumers have little if any means of effectively evading online tracking of their personal data. First and foremost, many providers of content and applications use “take it or leave it” privacy policy regimes. Furthermore, network and lock-in effects render switching from one service or application to another very difficult for consumers. For instance, consumers may agree to a privacy policy alteration of a social network site where most of their friends are registered, even if they disagree with its content. The most pressing problem, however, appears to be the evolution of difficult-to-evade tracking technology such as device fingerprinting. This type of tracking builds on the individual configuration of browsers and similar details of devices that are easily accessible from outside even without users noticing or using cookies.

On the other hand, the literature also indicates that consumers have developed strategies to at least evade targeted advertising, which is currently the major application of their tracked personal data. Specifically, the literature describes strategies of advertising avoidance and resistance. A longitudinal study of advertising avoidance indicates that there has been a noticeable shift from cognitive to mechanical avoidance of targeted advertising. Cognitive avoidance refers to consumers ignoring advertisements, while mechanical avoidance can be achieved by ad blockers, for instance.

A market for personal data that would give consumers the choice to either invest more time into managing their privacy or to pay for (more) privacy is sometimes suggested as a possible way to resolve the issues around personal data and privacy. Uncertainty about what actually happens with their personal data as well as potential consequences, however, impedes such a market.

Potential ways to improve informed consent in practice

Can terms and conditions be made more accessible?

Based on the premise that the opportunity costs of reading terms and conditions are the main reason that keeps consumers from engaging with them, one would conclude that making terms and conditions more accessible is likely to improve the likelihood of reading. In fact, various rules for the use of everyday language and concise information have been conceived as a means to reduce the time consumers have to spend reading terms and conditions. In line with this, web design and software tools have emerged to enable the development of intuitive and easy-to-use information and consent options. Furthermore, there are various studies that advocate the use of privacy labels similar to the ones used in food labelling to certify organic or fair trade product schemes. In light of studies demonstrating the misconceptions that such labels may trigger in consumers in relation to the protection of their personal data, such approaches may be debated. Nevertheless, the European Commission encourages the use of icons and the European Parliament has proposed requirements for companies to use icons to inform consumers about data-processing practices. There are signs that (in the UK at least) firms are becoming more pro-active as regards communicating their privacy notices. For instance, they are moving towards "just in time" notices that pop up at appropriate times.

Transparency fades with simplification.

Using her "transparency paradox", Nissenbaum addresses an even more fundamental issue with this concept, capturing the idea that "transparency of textual meaning and transparency of practice conflict in all but rare instances". This means that for a privacy policy to be actually transparent, the policy needs to be detailed and point out exactly who interacts with the data, when, how and to what end. However, this detail renders the texts so complex that no one reads them, let alone understands them.

Can consumer understanding be improved?

Multiple approaches to improve consumers' understanding have emerged. More harmonised information provisions may help reduce consumers' burdens for reading and understanding. Again, several researchers suggest using icons instead of text pop-ups or other condensed information. These icons generate trust when they embody a certification scheme. Furthermore, privacy policies that reflect a consumer's individual cultural background and preferences were found to contribute to better understanding. Other approaches shown to improve consumers' understanding use automated information extraction from privacy policies. Warnings about unexpected terms in a privacy policy may serve as a means to help consumers become aware of unusual

practices. Bashir et al.[1] integrate these ideas into their "Knowledge-based Individualized Privacy Plan" (KIPP). KIPP aims to improve consumer comprehension of the significance of privacy notices by personalising information based on different levels of pre-existing knowledge.

Can consumer action be ensured?

The insights presented so far call for a more contextualised and adaptive approach, which accounts for the possibility that both privacy policies and consumers' preferences may change over time. In line with this thought, "nudging" is one of the predominant ideas discussed among behavioural economists, psychologists and data protection representatives to help remind people of their choices and options continuously. Thus, it can trigger consumer action appropriate to the current context and preferences. As such, this may prevent consumers from making choices they might regret later. However, it has also been shown that too many such nudges may mitigate their effect.

Nudging consumers towards privacy is a "choice-preserving" approach. Consumers are free to make their own decisions but they are shown potential consequences of different privacy options. Other instruments to further consumer empowerment may complement nudging. Publishing opinions on privacy and protesting against unwanted changes in the terms and conditions of social networks, for example, may enhance consumer bargaining powers.

The impact of the Internet of Things (IoT)

More devices, more personal data.

Although data flows in the IoT do not differ fundamentally from the data flows observed in any connected environment, the sheer increase in the number of connected devices multiplies the data that becomes accessible and analysable. If expectations about the take-up of such connected devices are correct, online tracking of personal data is likely to become seamless across all areas of people's lives. Besides the increase in the amount of data, one may also expect that data gathering, aggregation and analysis will become even more subtle as machines talk to machines without (almost) any human intervention. Thus, consumers have even less opportunity to learn about data-gathering practices. In some cases, they may not even be aware that the device they are currently using is actually connected to the Internet.

1 Bashir, M.; Hoff, K.A.; Hayes, C.M.; Kesan, J.P. (2014): Knowledge-based Individualized Privacy Plans (KIPPs): A Potential Tool to Improve the Effectiveness of Privacy Notices, Workshop on the Future of Privacy Notice and Choice, Carnegie Mellon University June 27, 2014.

IoT aggravates issues around informed consent.

Consequently, it is likely that the evolution towards the IoT will aggravate the issues outlined in the present study for the status quo of connectivity. As regards the issue of reading terms and conditions, it is likely that the IoT will multiply the number and complexity of contractual relationships, which has to be reflected in the terms and conditions. These in turn are likely to become even longer and more difficult to understand. Furthermore, it is likely that many connected devices will feature only very small screens or even no screens at all. This will also render attempts to make such agreements easier to read, for example by turning them into a label, largely futile. Equally, nudging, albeit a promising approach in the current online environment, is unlikely to work with many connected devices. Finally, the IoT is likely to increase uncertainty about the consequences of consumers' actions because as the complexity of interactions multiplies, so do potentially adverse effects of willingly or unwillingly disclosing personal data.

Conclusion

There is no single solution for all issues yet.

The literature reviewed for the present study concurs as regards the dissonance between the assumptions and requirements stipulated in law about informed consent and actual consumer behaviour in practice. Consumers exhibit generally behaviour that is inconsistent with their stated concern for data privacy. As our study shows, insights from behavioural economics and in particular experimental studies can explain some of the reasons behind such behaviour as well as indicate potential ways to mitigate it. Context-aware nudging has emerged as a promising approach from the literature. However, nudging cannot solve all issues around informed consent at once. It seems that a single solution for all – or at least most – issues is yet to be found. Thus, more research appears to be necessary. Such research could investigate the extent to which a multi-faceted approach involving several factors in combination might offer potential solutions. In any case, further research should consider the IoT, whose evolution is likely to further aggravate the issues revolving around informed consent in practice.

Awareness may be the key.

In light of this development, as well as Helberger's[2] remark that consumer information is not a one-time act but a process, future research could perhaps address the phase of the consumer information process before they even come in contact with terms and conditions, namely when they become aware that there is an issue at all. Currently, there is a lot of uncertainty with consumers and experts alike regarding the potential

2 Helberger, N. (2013): Form Matters: Informing Consumers Effectively. Amsterdam Law School Research Paper No. 2013-71/Institute for Information Law Research Paper No. 2013-10.

effects of data collection. First, we have to be able to point to the specific (adverse) effects that may emerge from the tracking of personal data. Specific information about these effects is likely to raise awareness among consumers. This, in turn, is likely to motivate them to engage with terms and conditions and in particular privacy policies of services and products they consume. As the Elaboration Likelihood Model[3] predicts, higher motivation leads to more systematic and detailed information processing focusing on a high-quality argument instead of heuristic cues i.e. mental shortcuts. As a result, with increased awareness, consumers may be significantly more likely to actually engage with terms and conditions. Given this, this study presents some promising ways to facilitate the reading and understanding of terms and conditions as well as helping consumers make the right decisions at the right time.

Within this process, it should be taken into account that privacy is a fluid concept that has changed significantly over time. This can be illustrated by the early papers that have addressed the issue, which date back to the time when photography became more popular and was seen then as a significant threat to privacy and possibly society itself. Furthermore, future research should focus more on the cultural differences that exist related to the concept of privacy.

What we can learn from other disciplines.

Another potentially promising avenue for future research may be to learn from other disciplines that already have solutions to make informed consent work. We refer later to the example of clinical research, where it was first necessary to establish the actual risks if informed consent was not actual informed consent. It took a long list of – from today's perspective – unethical and quite frightening cases to come to the attention of researchers in the domain, courts and society at large before the domain could establish a notion of right and wrong, of what is ethical and that human trial subjects have rights after all. As much as it was a challenge for clinical research, it will be challenging for our domain to establish a widely acceptable understanding of relevant risks and benefits to consumers. However, if informed consent is to be the benchmark, there is no way around this debate in our domain. If the goal truly is that consumers make informed decisions, we can learn from clinical research that we have to make consumers understand and that we have to be able to specify relevant risks and benefits for consumers when they choose to use a digital and data-driven product or service.

3 Cacioppo, J. T.; Petty, R. E. (1983): Social psychophysiology: A sourcebook. Guildford Press.

Abbreviations

DPI	Deep Packet Inspection
e-Commerce	Electronic Commerce
e.g.	exempli gratia (for example)
et al.	et alii (and others)
ELM	Elaboration Likelihood Model
e-Privacy Directive	Electronic Privacy Directive
EU	European Union
EULA	End User Licence Agreement
GCP	Good Clinical Practice
HTML	HyperText Markup Language
IAB	Interactive Advertising Bureau
ICO	Information Commissioner's Office
i.e.	id est (in other words / that is)
IoT	Internet of Things
KIPP	Knowledge-based Individualized Privacy Plan
OECD	Organisation for Economic Co-operation and Development
PDF	Portable Document Format
SNS	Social networking site
UK	United Kingdom
US	United States
USA	United States of America
WHO	World Health Organization
WP29	The European Union's Article 29 Data Protection Working Party

1 Introduction

There are countless situations where our personal data is used to fulfil a service for us. For instance, a newspaper company requires subscribers' addresses to deliver the newspaper every morning. In this case, no further consent from subscribers is required for processing their addresses as the processing is a necessity to fulfil the contract they have entered into with the newspaper company. However, consent is often required for processing of personal data over and above the level that is necessary to fulfil the contract. In particular, with the increased use of the Internet, the use of mechanisms for user tracking such as cookies has come under scrutiny. On the one hand, such mechanisms enable online behavioural advertising, which in turn helps to enable most content or applications to be offered free of (monetary) charge to users.[4] On the other hand, such practices have been raising concerns among consumers and policymakers alike.

For instance, there is considerable uncertainty as regards who is gathering personal data and to what end. In turn, this may explain (sometimes vague) consumer fears and the fact that they value data privacy highly when asked in surveys about this subject. Actual behaviour, however, diverges substantially from reported importance. More often than not, consumers pay little or no attention to terms and conditions or more specifically privacy policies. This contradiction is commonly referred to as the "privacy paradox". It holds strong implications for the idea of informed consent and its consequences as consumers are likely to agree to terms and conditions they have not even read let alone understood, and thus they may later regret having given their consent. The number of situations when consumers consent to terms and conditions that they probably have not even read is increasing in line with the surging number of devices connected to the Internet and business models that in one way or another use personal data.

In order to respond accordingly, policymakers need to understand the dissonance between assumptions about and requirements for informed consent stipulated in law and actual consumer behaviour. While typically drawing on economic analysis resting on the assumption of fully rational consumer behaviour, the present issues require a broader perspective. Consequently, the present study set out to provide Ofcom with a broad literature review that gathers insights from behavioural economics, consumer behaviour research, information processing, law and psychology. Wherever relevant, insights from existing regulation and legislation are also integrated.

---

4 Arnold, R.; Waldburger, M. (2014): The Impact of Data on ICT Business Models. GSR Discussion Paper. Available at: http://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2014/GSR14%20Impact_of_dataBusinessModels.pdf.

The literature review aims to gain an understanding of (1) the role of informed consent in privacy law, (2) the role of informed consent in practice and (3) potential ways to improve informed consent in practice. The remainder of the report is structured around these three subjects. It culminates in a concluding chapter that summarises the major findings from the preceding literature review and identifies gaps in the existing research. Based on this analysis, we make suggestions for avenues for possible future research.

The study adopts a European angle with respect to the role informed consent plays in privacy law. The literature review on informed consent in practice focuses on empirical insight. It covers primarily studies that obtain their results from trials and experiments. It is due to this scope that the present study does not provide a detailed discussion of guidelines on privacy and informed consent, such as the Federal Trade Commission's Fair Information Practice Principles[5] and its 2012 recommendations[6], the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[7], the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[8], or the European Commission's Data Protection and Privacy Ethical Guidelines[9]. As regards informed consent's (future) role in law, the study mentions current efforts in Europe to create a digital single market, which entails a reform of European data protection law, but it refrains from a deepened analysis, since the reform is ongoing and the outcome is difficult to anticipate.[10]

Whilst the present study draws from numerous research fields, it does not discuss the concept of privacy as such. It should, however, be noted that this concept is all but static over time. For instance, the earliest research papers on privacy date back to the advent of photography and the fear of how this may invade the individual's private sphere. In line with this, we also do not specifically discuss what personal data is exactly, but stick to the definition provided by Ofcom[11]:

- "Volunteered data comes directly from the individual – photos, blogs, tweets, videos, comments, "likes", e-mail messages and so on.

5 Federal Trade Commission (1998): Privacy Online: A Report to Congress: 1-63. And: Federal Trade Commission (2000): Privacy Online: Fair Information Practices in the Electronic Marketplace. A Report to Congress: 1-56.
6 Federal Trade Commission (2012): Protecting Consumer Privacy in an Era of Rapid Change. Recommendations for Businesses and Policymakers: 1-74.
7 OECD (1980): OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. And: OECD (2013): The OECD Privacy Framework: 1-154.
8 Council of Europe (1981): Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.
9 European Commission Experts Working Group on Data Protection and Privacy (2009): Data protection and privacy ethical guidelines: 1-18.
10 For a critical approach on informed consent and data protection see Custers, B.; van der Hof, S.; Schermer, B.; Appleby-Arnold, S.; Brockdorff, N. (2013): Informed Consent in Social Media Use – The Gap between User Expectations and EU Personal Data Protection Law. Oben access article published in SCRIPTed.
11 Definition quoted from the Tender Specifications.

- Observed data is created as a result of a transaction between an individual and an organization – location data from a mobile phone, credit card transactions, purchase history at a retailer, etc.
- Inferred data, also called derived data, is the output of data analysis, combination or mining, and it includes credit scores, predictions of preferences and purchase intent.“

Finally, it should be noted that this literature review is not meant to be an exhaustive representation of all the literature that is available on the topic. The papers selected for this review were chosen based on their relevance to the specific question we intend to answer. Generally, more recent papers were preferred over less recent ones. Nonetheless, the seminal works in the area were covered.

2 The role of informed consent in privacy law[12]

2.1 Fundamental rights and general data protection law

Consent plays a central role in most data privacy laws in the world.[13] With respect to online marketing practices, it is important to realise that in Europe informed consent is needed both for placing cookies or similar tracking devices on user's computers, according to the e-Privacy Directive, as well as for ensuing collection and processing of personal data, as regulated by the Data Protection Directive. There are instances in which consent is not required, e.g. if a cookie is necessary for transmission of communication, or for a service explicitly requested by the user. Furthermore, many personal data processing activities can be based on another legal basis than the data subject's consent. For instance, if the fulfilment of the specific service requires processing of personal data, consent is not always required. Nevertheless, consent plays a central role in the rules for online data processing.

The right to privacy is protected in various treaties.[14] In Europe, the right to privacy is included in Article 8 of the European Convention on Human Rights.[15] The European Court of Human Rights holds that the right to privacy protects people's Internet use against surreptitious monitoring: "the Court considers that the collection and storage of personal information relating to the applicant's telephone, as well as to her e-mail and Internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8."[16]

In Europe, one of the main legal instruments to protect privacy and related interests in the context of digital data processing is data protection law. The right to protection of personal data is a fundamental right in the European Union, and is included in the 2000 Charter of Fundamental Rights of the European Union (legally binding since 2009). Article 8 of the Charter says: "Everyone has the right to the protection of personal data concerning him or her."[17] The second paragraph of Article 8 illustrates the important role of consent: "Such data must be processed fairly for specified purposes *and on the basis of the consent of the person concerned* or some other legitimate basis laid down by law" (emphasis added).

---

12 This chapter has been written by Frederik Zuiderveen-Borgesius, Institute for Information Law (IViR), University of Amsterdam.

13 For general principles on the principles of data privacy law in the world, see: Bygrave L. A. (2014): Data privacy law. An international perspective. Oxford University Press, chapter 5; Greenleaf, G. (2013): Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories. Journal of Law, Information & Science 23(1).

14 See for instance Article 17 of the International Covenant on Civil and Political Rights; Article 12 of the UN Declaration of Human Rights.

15 Article 8.

16 ECtHR, Copland v. United Kingdom, No. 62617/00, 3 April 2007, par 44. Please note, this is a direct quote from the Court's Judgement and refers, with respect to the case of telephone, to information relating to the date and length of telephone conversations and in particular the numbers dialled.

17 Article 8(2) of the Charter of Fundamental Rights of the European Union.

In daily practice, the national implementation law of the 1995 Data Protection Directive, such as the Data Protection Act 1998 in the UK, is most relevant. In the following text, we will concentrate on a description of the Data Protection Directive, which has laid the ground for national data protection laws in Europe, including that of the UK.

The Data Protection Directive only allows personal data processing if an organisation or company using personal data ("data controller"[18]) has a legal basis for the processing.[19] For companies processing personal data, the most relevant legal bases are Article 7(b), processing of personally data is a necessity for the performance of a contract between data controller and data subject, Article 7(f), according to which the processing must be necessary for the purposes of the legitimate interests pursued by the controller or by the third party to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject; and Article 7(a), i.e. the case that the data subject has given its unambiguous consent into the processing.[20]

For many personal data processing practices, no unambiguous consent is needed because one of the other legitimate reasons applies. For example, for a newspaper subscription, processing some personal data is necessary; the subscriber's address is necessary to deliver the newspaper. Hence, to process the subscriber's address, the newspaper company can rely on the legal basis of necessity for contract performance. The company does not have to ask the subscriber for separate consent for the use of the subscriber's address, as long as the company only uses that personal data to perform the contract.

For many innocuous standard business practices, a company can rely on the balancing provision. The balancing provision allows personal data processing, in short, if the company's interests outweigh the data subject's interests and privacy rights.[21] For example, a shop can send an existing customer paper brochures for the same type of products the customer bought before (i.e. first-party direct mail marketing).

If a company wants to process personal data, and cannot base the processing on the balancing provision or on another legal basis, only the data subject's "unambiguous consent" is required.[22] The Data Protection Directive defines consent as "any freely

18 The data controller is the "body which alone or jointly with others determines the purposes and means of the processing of personal data" (article 2(c) of the Data Protection Directive). The Directive distinguishes data processors (article 2(e)) from controllers. This report leaves that complication aside, and speaks of "company" for ease of reading.

19 Article 6(1)(b) of the Data Protection Directive requires a "legitimate purpose"; the literature usually speaks of a "legal basis". Article 7 lists the six possible legal bases for personal data processing.

20 The data subject is the person that personal data refer to (article 2(a) of the Data Protection Directive).

21 Article 7(f) reads as follows: "Member States shall provide that personal data may be processed only if: (…) (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1)."

22 Article 7(a) of the Data Protection Directive.

given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."[23] Consumers can always withdraw their consent.[24]

An indication of wishes can be given in many ways, and also implicitly. For instance, somebody can indicate his or her wishes by clicking an "I agree" button. However, an indication of wishes does require an expression of will.[25] Mere silence or inactivity of the data subject can generally not be interpreted as an expression of will.[26] This implies that opt-in systems are generally required for valid consent. With an opt-out system, where a data subject is presumed to "consent" if he or she does not object, there would almost never be an indication of wishes, as required by Article 2(h) of the Data Protection Directive ("unambiguous consent").

Furthermore, consent must be "informed" and "specific" to be valid. The controller must supply the data subject with the information s/he needs, such as the name and address of the controller, the processing purpose, the data recorded, etc.[27] The requirement that consent must be "specific" means that a consent request must concern "a particular data processing operation concerning the data subject carried out by a particular controller and for particular purposes".[28]

While consent plays an important role in data protection law, that role should not be exaggerated. First, as discussed in the above, for many personal data processing activities the law does not require prior consent, notably those covered by the other legitimate grounds in Article 7(b) and (f) of the Data Protection Directive (necessary for the performance of a contract or justified by a legitimate interest of the data controller that outweighs the data subject's interests). Second, even if a company has a legal basis for personal data processing, such as data subject consent or the balancing provision, the company must still comply with all the other requirements that follow from the Data Protection Directive.[29] In other words, even after the data subject has given his or her unambiguous consent for personal data processing, all the other data

---

23 Article 2(h) of the Data Protection Directive.

24 1992 EC COM (92) 422 final amended proposal Data Protection Directive, p. 12.

25 See: Article 29 Working Party, "Opinion 15/2011 on the definition of consent" (WP 187) 13 July 2011.

26 Likewise, in general contract law, mere silence does not constitute an indication of will. See for instance Article 18(1) of the Vienna Sales Convention: "[a] statement made by or other conduct of the offeree indicating assent to an offer is an acceptance. Silence or inactivity does not in itself amount to acceptance."

27 1992 EC COM (92) 422 final amended proposal Data Protection Directive, p. 11. "To enable the data subject to make an assessment of the advantages and disadvantages of the processing of data concerning him, and to exercise his rights under Article l3 of the proposal (rectification, erasure and suppression), the consent given must be informed. The controller must supply the data subject with the information he needs, such as the name and address of the controller and of his representative if any (see Article 4(2)), the purpose of the processing, the data recorded, etc."

28 1992 EC COM (92) 422 final amended proposal Data Protection Directive, p. 12.

29 See: Court of Justice of the European Union, Case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos and Mario Costeja González, not yet published, par. 71: "all processing of personal data must comply, first, with the principles relating to data quality set out in Article 6 of the directive and, secondly, with one of the criteria for making data processing legitimate listed in Article 7 of the directive (…)".

protection requirements still apply. For example, even after consent, companies may not process disproportionate amounts of personal data;[30] must secure the data they hold;[31] and may not use personal data for new purposes at will.[32]

Informed consent in the Data Protection Directive

- *Consent plays an important role in most data privacy laws in the world. The national implementation law of the 1995 Data Protection Directive is most relevant in the UK.*
- *Personal data processing requires a legal basis. For the private sector, consent, necessity for contract performance, and the balancing provision are the most important legal bases. Data subject consent is not required if personal data processing is a necessity for contract performance. Consent is also not required if processing is necessary for the legitimate interests of a company which processes personal data, and those interests are not overridden by the data subject's privacy rights.*
- *After the data subject's consent, data protection law as regards to e.g. the scope and period of data processing still applies in full.*

2.2 Informed consent in the e-Privacy Directive

Consent plays an especially important role in an online context. Article 5(3) of the 2009 e-Privacy Directive requires, in short, parties to obtain the user's consent before storing or accessing information on a user's device (subject to exceptions).[33] For the definition of consent, the e-Privacy Directive refers to the Data Protection Directive's consent definition: a freely given, informed and specific indication of wishes.[34]

Article 5(3) has several rationales. First, a user's devices, such as phones or computers, and the contents of those devices, are part of the user's private sphere as protected by the European Convention on Human Rights.[35] Therefore, such devices and their contents, such as saved messages, address books, etc., should not be read or accessed without the user's consent. Second, Article 5(3) protects users against placing spyware, tracking devices or other software on the devices without their

30 Article 6(1)(c) and 6(1)(e) of the Data Protection Directive.
31 Article 17 of the Data Protection Directive.
32 Article 6(1)(b) of the Data Protection Directive.
33 Article 5(3) of the e-Privacy Directive, amended in 2009.
34 Article 2(f) of the e-Privacy Directive refers to the Data Protection Directive.
35 Recital 24 of the e-Privacy Directive.

consent.[36] Third, Article 5(3) aims to protect people against surreptitious tracking of their activities.[37]

Article 5(3) also applies to storing and accessing cookies on people's devices. This application of Article 5(3) has received most attention in the recent debate. In brief, Article 5(3) requires consent for cookies, unless the cookie is necessary for transmission of communication, or for a service explicitly requested by the user. This implies, for instance, that no prior consent is required for using cookies for log-in procedures, for digital shopping carts or for language preferences.

The "indication of wishes" requirement has led to much discussion in the context of consent for cookies. While for instance the UK's ICO (Information Commissioner's Office) recommends opt-in boxes over other methods such as opt-out boxes, the ICO acknowledges with reference to the e-Privacy Directive that an opt-in box "is not necessarily the only way of obtaining consent".[38] This situation of ambiguity may have given support to claims that opt-out systems may be used to obtain "implied" consent. Some companies suggest people give consent to all types of cookies, including tracking cookies, if they have not changed the default settings on their browsers.[39]

The opt-in/opt-out discussion regarding cookies is likely caused by several factors. First, a recital of the 2009 Directive that amended the e-Privacy Directive says: "Where it is technically possible and effective, in accordance with the relevant provisions of [the general Data Protection Directive], the user's consent to processing may be expressed by using the appropriate settings of a browser or other application."[40] Some conclude that a user's default browser settings can express consent.[41] That interpretation has not been confirmed in case law. The interpretation seems hard to reconcile with the requirements of the Data Protection Directive, among other reasons because the recital

---

36 Recital 24 of the e-Privacy Directive. "So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users."

37 Recital 24 of the e-Privacy Directive: "hidden identifiers (…) can enter the user's terminal without their knowledge (…) to trace the activities of the user and may seriously intrude upon the privacy of these users." Recital 65 of Directive 2009/136: "Software that surreptitiously monitors the actions of the user or subverts the operation of the user's terminal equipment to the benefit of a third party (spyware) poses a serious threat to the privacy of users, as do viruses."

38 Information Commissioner's Office (2013): Direct marketing. Data Protection Act. Privacy and Electronic Communications Regulations. Version 1.1, p 17-18.

39 See e.g. Internet Advertising Bureau United Kingdom, "Department for Business, Innovation & Skills consultation on implementing the revised EU electronic communications framework, IAB UK Response" (1 December 2012) www.iabuk.net/sites/default/files/IABUKresponsetoBISconsultationonimplementingtherevisedEUElectronicCommunicationsFramework_7427_0.pdf, p 2.

40 Recital 66 of Directive 2009/136.

41 See e.g. Internet Advertising Bureau United Kingdom, "Department for Business, Innovation & Skills consultation on implementing the revised EU electronic communications framework, IAB UK Response" (1 December 2012) www.iabuk.net/sites/default/files/IABUKresponsetoBISconsultationonimplementingtherevisedEUElectronicCommunicationsFramework_7427_0.pdf, p 2.

refers to the Data Protection Directive, which requires an indication of wishes for consent.

Second, the scope of Article 5(3) has proven to be too broad in practice. For instance, Article 5(3) also requires consent for some website analytics cookies, as the provision does not contain an exception for such cookies. But it seems overly burdensome if website publishers must ask consent to use analytics cookies. And Internet users would likely not appreciate having to click "I agree" every time a website wants to use analytics cookies. The Article 29 Working Party, in which national data protection authorities cooperate, has suggested introducing an exception in the e-Privacy Directive for privacy-friendly analytics cookies, i.e. cookies that are strictly limited to the collection of first party anonymized and aggregated statistical purposes.[42]

Third, many websites allow third parties such as advertising networks to place tracking cookies, for instance for targeted marketing. Such websites might make less profit if they had to ask visitors for consent for placing such tracking cookies as visitors might not consent.

There are some variations in the way in which European Union member states have chosen to implement Article 5(3) at the national level. For instance, Ireland allows opt-out systems for obtaining consent for cookies, even though an active indication of wishes is lacking with such opt-out systems.[43]

Informed consent in the e-Privacy Directive

- *The e-Privacy Directive requires companies to obtain consent for placing or reading most types of cookies (and similar computer files) used for tracking purposes.*
- *There is an on-going discussion about how consent should be obtained.*

42 Article 29 Working Party, „Opinion 04/2012 on Cookie Consent Exemption" (WP 194) 7 June 2012, p. 10-11.

43 The Irish implementation of Article 5(3) says: "5. (1) A person shall not use an electronic communications network to store information, or to gain access to information stored in the terminal equipment of a subscriber or user, unless (…) (b) the subscriber or user is offered by the data controller the right to refuse to consent to that use." Irish Statutory Instrument (S.I.) No. 535 of 2003 as amended by S.I. No. 526 of 2008 www.dataprotection.ie/viewdoc.asp?DocID=896 .

2.3 Future developments

Data protection law continues to evolve. In 2012, the European Commission published a proposal for a data protection regulation to replace the 1995 Data Protection Directive. Again, consent plays a central role in the proposal. The 2012 proposal always requires consent to be "explicit". That requirement has led to much lobbying; apparently, many companies prefer weaker requirements for consent.[44] The proposal is still being discussed in Brussels with negotiations probably ending in June 2015.[45] It is unclear, however, whether the proposal will be adopted in 2015.[46]

Technology also evolves. For instance, more objects are being connected to the Internet, leading to an "Internet of Things" (IoT). In IoT scenarios, the general Data Protection Directive and the e-Privacy Directive apply to many situations. The Data Protection Directive applies when "personal data" is processed; this is often the case in IoT settings.[47] For instance, if an Internet-connected refrigerator automatically orders groceries, some personal data such as the customer's delivery address must be processed to deliver groceries. The companies processing that data must comply with data protection law. If they want to use the personal data for more purposes than grocery delivery, they must, in many cases, obtain the data subject's consent.

Article 5(3) also requires companies to obtain the user's consent if companies access information on a user's device. The Article 29 Working Party gives the following example:

"A pedometer records the number of steps made by its user and stores this information in its internal memory. The user installed an application on his computer to download directly the number of steps from his device. If the device manufacturer wants to upload the data from the pedometers to its servers, he has to obtain the user's consent under Article 5(3) of directive 2002/58/EC [the e-Privacy Directive]."[48]

---

44 For instance, Facebook proposes deleting the phrase "Silence or inactivity should therefore not constitute consent." (Facebook recommendations on the Internal Market and Consumer Affairs draft opinion on the European Commission's proposal for a General Data Protection Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data" https://github.com/lobbyplag/lobbyplag-data/raw/master/raw/lobby-documents/20121026_Drafting-recommendations_IMCO-draft-opinion_final.pdf).

45 Lexology visited on 21-05-2015, see: http://www.lexology.com/library/detail.aspx?g=089098fa-41fd-461d-87dc-969584e8302d.

46 See: Privacylaws.com, "Albrecht optimistic about 2015 deadline for EU DP Regulation" (23 January 2015) www.privacylaws.com/Int_enews_23_1_15.

47 IoT devices often process both personal data and data that does not qualify as personal data.

48 Article 29 Working Party, "Opinion 8/2014 on the Recent Developments on the Internet of Things" (WP 2234) 16 September 2014, p. 14.

Future developments

- *Informed consent plays a major role in data privacy law, and it will continue to play an important role in the future.*
- *The legal basis "consent" is often applicable in IoT situations.*

3 The role of informed consent in practice

3.1 Do consumers read?

The premise that consumers read contractual agreements they sign is evidently the very cornerstone of the informed consent principle. Consequently, it is not surprising that there is a long-standing and well-established stream of research that has aimed to answer the question of whether consumers actually do read the agreements they sign. The studies published in this stream of research concur that consumers sign all sorts of contractual agreements without reading them.[49] It is, however, important to differentiate by contractual subject matter. For instance, mundane activities such as bank transactions appear to draw less readership (only 8% of respondents stating that they read the terms and conditions), while an activity that affects a dependent child such as signing a nursery contract would be read by 76% of respondents.[50]

The "clicking-without-reading" phenomenon in the online environment can be understood as an extension of the signing-without-reading problem apparent in the offline sphere. The most prominent study confirming this thesis as regards consumers' online behaviour is the one performed in 2007 by Bakos et al.[51] They tracked the online behaviour of 45,091 US households across 66 software companies to explore how many potential buyers accessed the so-called EULAs (End User Licence Agreements). Across 120,545 observations, only 55 incidents were registered where consumers actually accessed these EULAs. Even more surprisingly, potential buyers who accessed the respective EULA spent on average only 47.7 seconds reading it. In essence, it is fair to say that practically no potential buyer actually read the EULAs. It is

49 Bakos, Y.; Marotta-Wurgler, F.; Trossen, D.R. (2009): Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts. NYU Law and Economics Research Paper No. 09-40; Becher, S. L. Unger-Aviram, E. (2010): The Law of Standard Form Contracts: Misguided Intuitions and Suggestions for Reconstruction. DePaul Business & Commercial Law Journal, Vol. 8: 199-227; De Geest, G. (2002): The signing-without- reading problem: An analysis of the European Directive on unfair contract terms, in H. B. Schäfer & H. J. Lwowski (Eds.), Konsequenzen wirtschaftsrechtlicher Normen Festschrift für Klaus Ott (pp. 213–235). Wiesbaden: Gabler; Maronick, T. J. (2014): Do Consumers Read Terms of Service Agreements When Installing Software? A Two-Study Empirical Analysis. International Journal of Business and Social Research 4(6): 137-145. Stark, J. K.; Choplin, J. M. (2009): A License to Deceive: Enforcing Contractual Myths Despite Consumer Psychological Realities. 5 N.Y.U. J. L. & Bus: 617. Jensen, C.; Pottsa, C.; Jensen, C. (2005): Privacy practices of Internet users: Self-reports versus observed behaviour. Int. J. Human Computer Studies 63: 203-227. European Consumer Centre Ireland (2008): Car Rental Contracts: Business practices, contract terms and consumer protection. Dublin. Cranor, L. F.; Hoke, C.; Leon, P. G.; Au, A. (2014): Are They Worth Reading? An In-Depth Analysis of Online Advertising Companies' Privacy Policies. Non-reviewed draft paper presented at the 42nd Research Conference on Communication, Information and Internet Policy (TPRC 2014).

50 Becher, S. L. and Unger-Aviram, E. (2010): The Law of Standard Form Contracts: Misguided Intuitions and Suggestions for Reconstruction. DePaul Business & Commercial Law Journal, Vol. 8: 199-227.

51 Bakos, Y.; Marotta-Wurgler, F.; Trossen, D.R. (2009): Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts. NYU Law and Economics Research Paper No. 09-40. Recently this work was also published in the Journal of Legal Studies 43(1). See also Wilkinson-Ryan, T. (2014): A Psychological Account of Consent to Fine Print. Institute for Law and Economics at the University of Pennsylvania, Research Paper No. 14-22.

important to note that Bakos et al. were able to track actual consumer behaviour. As a result their findings cast severe doubts on surveys that rely on consumer reports about their own behaviour. For instance, in a recent survey in Canada, only 24% report that they never read such policies.[52] Similarly, the most recent German D21 survey[53] finds that 52% of Germans claim they read the terms and conditions of websites they visit. Given that it is widely established in consumer behaviour research that stated behaviour often diverges significantly from actual behaviour,[54] we consider the results by Bakos et al. very useful in understanding actual consumer behaviour in relation to EULAs. We have no indication to think that the difference between stated and actual behaviour is likely to be any different for privacy policies.

The predominant reason for consumers signing or clicking without reading contracts in various situations is the time taken to go through pages and pages of text.[55] Two studies[56] have addressed the issue of opportunity costs (costs incurred by missed opportunities) incurred by reading privacy policies or permissions in detail. They concur in their assessment that these costs for consumers would be significant. The study by McDonald and Cranor draws on empirical evidence referring to the average length of privacy policies, reading speed and the number of websites visited. They calculate that it would take a web user several weeks per year to read the privacy policies on each website they visit.[57] Given that the paper refers to data from 2007, it is likely that their

52 Phoenix Strategic Perspectives (2013): Survey of Canadians on Privacy-Related Issues. Prepared for the Office of the Privacy Commissioner of Canada.

53 D21 Initiative (Ed.) (2014): D21-Digital-Index 2014. Die Entwicklung der digitalen Gesellschaft in Deutschland. Berlin. Another representative study ten years ago by the German consumers association (vzbv) suggests that consumers ignore most of the information offers but would not like to renounce any information, see Schoenheit, I. (2004): Was Verbraucher wissen wollen. Ergebnisse und Thesen zu einer empirischen Studie. Berlin.

54 Callegaro, M. (2008): Social desirability. P. Lavrakas (Ed.), Encyclopedia of survey research methods. (pp. 826-827). Thousand Oaks, CA: SAGE Publications, Inc. For instance, social desirability often leads consumers to report actions that are generally perceived to be positive or otherwise socially desired. This is very likely also the case here. Reading terms and conditions can be understood as socially desirable behaviour.

55 The situation is certainly not improved by the technical (often legal) jargon these texts use. Whether consumers understand the terms and conditions is addressed in the following section.

56 McDonald, A. M.; Cranor, L. F. (2008): The Cost of Reading Privacy Policies. A Journal of Law and Policy for the Information Society 4(3) I/S: 540 and Sarode, S. (2014): Opportunity cost analysis of android smartphones' permissions. Master Thesis at the Rutgers University New Brunswick. The study by Sarode addressed the issue of opportunity cost by reference to the permission statements of smartphone apps on Android-based mobile devices. As compared to websites (which were looked at in the study by McDonald and Cranor), statements used for smartphone apps are commonly presented in both a short and a detailed version. Sarode's study accounts for this effect as well as the effect of consumers learning to read and understand such permissions and thus becoming quicker at reading them. He estimated that reading the short versions of all terms and conditions for apps a consumer installs over a year (on average) accumulates opportunity costs of $23 when done at work or $3 when read during leisure time. If consumers were to read the detailed versions of such permissions, the cost would amount to $106 or $13, respectively. While these results indicate that with mobile devices and apps, the opportunity cost of reading is declining as presentation on small screens necessitates shorter statements, it should be noted that the use of smartphones and other mobile devices increases total time spent online. Consequently, it is likely that the total cost of reading privacy policies is increasing too.

57 To put consumers' costs of reading in perspective, researchers tend to compare the cost to consumers in terms of their time with the revenue generated by online advertising at the time the study is carried out. Such a comparison shows that online advertising revenue is substantially lower

results would now underestimate the current opportunity costs occurring for Internet users as the time spent on the Internet and the number of visited websites have likely increased since then.

Besides the cost associated with reading privacy policies for consumers, there is also a more obvious observation to make in the context of websites. A Chartbeat analysis of 2 billion page visits across the Internet found that 55% of users spent less than 15 seconds actively on a page.[58] Furthermore, around a fifth of mobile apps that consumers download are used only once.[59] In light of the Chartbeat figures, there is understandably little incentive for consumers to spend time reading privacy policies as this is likely to consume significantly more time than they actually spend using the content or the application they want to use.

As indicated in the studies cited at the beginning of this section, consumers prefer to allocate their time to activities other than reading terms and conditions in most situations. When surfing the web or consuming other online services, several factors may facilitate ignoring terms and conditions. The following paragraphs discuss such factors.

First and foremost, it is significantly easier for consumers to ignore the terms and conditions when they are surfing the web. Unlike in financial services, medical care or large purchases (such as a car), there is no one there to point them to the terms and conditions and no physical signature is required. Consenting is further facilitated by presenting consumers more often than not with a pre-set default option when they are asked to agree to the terms and conditions. Setting the default option to “agree” is likely to build on a cognitive bias that is well established in the literature on human behaviour, namely the status quo bias. Originally identified by Samuelson and Zeckhauser’s study on decision-making,[60] humans’ tendency to stick to the default option has been documented in numerous studies across various fields of investigation.[61] Presumed

---

than the opportunity costs associated with reading the relevant terms and conditions that (technically) enable online advertising in the first place – despite a sharp increase in online advertising revenue. For instance, expressed in dollars, the opportunity cost to consumers of reading would be around $781 billion. In contrast total online advertising revenue in the United States was estimated to be $21billion in 2007. McDonald, A. M.; Cranor, L. F. (2008): The Cost of Reading Privacy Policies. A Journal of Law and Policy for the Information Society 4(3) I/S: 540.

58 cf. Halle, T. (2014): What You Think You Know About the Web Is Wrong. TIME 03-09-2014. Available at: http://time.com/12933/what-you-think-you-know-about-the-web-is-wrong/

59 Localytics (2014): App Retention Improves – Apps Used Only Once Declines to 20%. 06-11-2014. Available at: http://info.localytics.com/blog/app-retention-improves

60 Samuelson W. and Zeckhauser, R. (1988):): Status Quo Bias in Decision Making. Journal of Risk and Uncertainty. Volume 1(1): 7. For another description of this phenomenon in the context of privacy see also Zuiderveen Borgesius, F. J. (2015): Improving Privacy Protection in the Area of Behavioural Targeting (PhD thesis University of Amsterdam), Kluwer law International (forthcoming).

61 Shah, R. C. and Sandvig, C. (2008): Software Defaults as de facto Regulation: The case of the wireless internet. Information, Communication & Society 11(1): 25-46; Goldstein, D.G.; Johnson, E.J.; Hermann, A. and Heitmann, M. (2008): Nudge your customers towards better choices. Harvard Business Review 86(12): 99-105.; Johnson, E.J. and Goldstein, D. (2003): Do defaults save lives? Science 302(5649): 1338-1339.; Jin, L. (2011): Improving response rates in web surveys with default setting: The effects of default on web survey participation and permission. International Journal of Advertising 53(1): 75-94.

consent to organ donation legislated in several European countries can be taken as an intuitive example of status quo bias. Very few people actually opt out of presumed consent to organ donation just as most people do not opt into organ donation if it is not the "default option" in their country of residence. Abadie and Gay[62] find in their cross-country study that presumed consent to cadaveric organ donation in fact explains much of the variation in actual donation rates across countries.

In the case of "browse-wrap" contracts, consumers agree to the terms and conditions simply by using the website or the respective application. Turow[63] and Kim[64] state that such settings indicate that many websites actually do little to encourage consumers to read terms and conditions.

Another relevant aspect to consider is that there is little awareness among consumers about targeted advertising practices and what happens with their personal data when they surf the web or use a mobile app. In fact, this lack of knowledge may incline consumers to believe that nothing bad happens by not reading privacy policies. Interestingly, consumers display the behaviour of not reading privacy policies despite reporting consistently high concern for the protection of their private data.[65] This is likely to be due to strong information asymmetry in the market. For instance, web users are commonly surprised to learn that their browsing history is analysed and used for targeted advertising. This is documented in studies by Ur et al. [66] and Cranor and McDonald.[67] The latter found that significantly less than half of web users (40%) were aware that their emails may be scanned to enable targeted advertisements. The "discrepancy between attitudes and behaviors"[68] phenomenon is referred to as the "privacy paradox". Furthermore, 29% of users in the same study did not believe that this was actually common practice as they thought such practices would be unlawful. These results may be taken as an indication that consumers do not have the (ex-ante) knowledge to make informed decisions about privacy.

---

62 Abadie, A. and Gay, S. (2006): The impact of presumed consent legislation on cadaveric organ donation: A cross-country study. Journal of Health Economics 25(4): 599-620.

63 Turow, J. (2001): Privacy Policies on Children's Websites: Do They Play by the Rules? The Annenberg Public Policy Center, March 2001.

64 Kim, N. (2010): Wrap Contracts and Privacy. Association for the Advancement of Artificial Intelligence. Press Technical Report SS-10-05.

65 For instance: Rao, A.; Schaub, F.; Sadeh, N. (2014): What do they know about me? Contents and Concerns of Online Behavioral Profiles. 2014 ASE BigData/SocialInformatics/PASSAT/ BioMedCom Conference, Harvard University, December 14-16, 2014: Conference Full Papers.

66 Ur, B.; Leon, P.G.; Cranor, L. F.; Shay, R.; Wan, Y. (2012): Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising. Proceedings of the Eighth Symposium on Usable Privacy and Security ACM, p 4. The interviews were conducted in the United States. There is little evidence that consumers in Europe in 2014 have a better understanding of behavioural targeting.

67 McDonald, A.M.; Cranor, L.F. (2010): Beliefs and Behaviors: Internet Users. Understanding of Behavioral Advertising (38th Research Conference on Communication, Information and Internet Policy (Telecommunications Policy Research Conference)) (2 October 2010).

68 Acquisti et al. explain the "privacy paradox" in a recent review of empirical reserach in this field, Acquisti, A.; Brandimarte, L.; Loewenstein, G. (2015): Privacy and human behavior in the age of information. Science 347(6221): 509-514. An early experiment as regards the privacy paradox was conducted by Acquisti et al. in the year 2004: Acquisti, A.; Grossklags J. (2005): Privacy and rationality in individual decision making. IEEE Security & Privacy 3(1) 26-33.

Frequent changes in privacy policies of websites, services and products may even hinder consumers who have found ways to escape such tracking under the respective terms and conditions. For instance, many companies reinstall cookies that have already been deleted. Furthermore, consumers may not be aware of the long-term consequences. Most often websites are used only for a short amount of time. The same is true for many mobile apps.[69] However, tracking of the consumers' personal data may continue long after their use of the website or app. Consequently, Hoofnagle et al. summarise that "advertisers are making it impossible to avoid online tracking".[70]

Other studies indicate that consumers are adapting their behaviour. Rader[71] finds that awareness of online tracking practices is high among web-savvy consumers. Interestingly, these consumers appear to be less concerned about the consequences of their data being collected, analysed and used.

Kelly's PhD thesis[72] documents several advertising avoidance strategies used by consumers. Her participants consisted of young adults that took part in a qualitative four-year cohort study. Participants showed significant changes in their perceptions of privacy on social networking sites (SNSs) as regards targeted advertising as well as advertising avoidance strategies. While in the first study (2007) participants mainly used cognitive avoidance strategies, i.e. ignoring the advertisements, in 2011, they also started to use mechanical avoidance through advertisement blockers. In the second study, advertising on YouTube came across as particularly annoying since it cannot be blocked. Consequently, participants tended to open a different tab while the advertisement ran on YouTube. As regards affective advertising avoidance, participants showed a dislike for the advertisements they received on their SNSs in both studies. However, while in the first study they were more annoyed by the fact that advertising did not match their preferences at all, in the second study they were annoyed when advertisements were actually too close to their preferences.

---

69 Around 20 % of apps are used only once after they have been downloaded (Localytics (2014): App Retention Improves – Apps Used Only Once Declines to 20%. 06-11-2014. Available at: http://info.localytics.com/blog/app-retention-improves). For a recent study on tracking in mobile networks see e.g. Eubank, C.; Melara, M.; Perez Botero, D.; Narayanan, A. (2013): Shining the Floodlights on Mobile Web Tracking – A Privacy Study. Proceedings of the IEEE Workshop on Web 2.0.

70 Hoofnagle, C.J. et al (2012): Behavioral Advertising: The Offer You Cannot Refuse. 6(2) Harvard Law & Policy Review, 273. Cf. Zuiderveen Borgesius, F. J. (2015): Improving Privacy Protection in the Area of Behavioural Targeting (PhD thesis University of Amsterdam), Kluwer law International (forthcoming).

71 Rader, E. (2014): Awareness of Behavioral Tracking and Information Privacy Concern in Facebook and Google. Symposium on Usable Privacy and Security (SOUPS) 2014, July 9–11,2014, Menlo Park, CA.

72 Kelly, L.M.V. (2014): An Exploration of Advertising Engagement, Advertising Avoidance and Privacy Concerns on Social Networking Sites. PhD Thesis at the School of Advertising, Marketing and Public Relations – QUT Business School. Queensland University of Technology – November 2014. For more detail on advertising avoidance, please refer to section 3.3.

Do consumers read?

- *The "clicking-without-reading" phenomenon is widespread for terms and conditions in the online environment. There is a notable difference in consumers' stated and actual behaviour.*
- *Reading terms and conditions requires too much time. Consumers refrain from reading them because of the opportunity cost.*
- *Ignoring terms and conditions is significantly easier in the online than in the offline world as there is no one to point consumers to the terms and conditions and no physical signature is required.*
- *As a result, information asymmetries remain stable: website providers know much more about their data protection policies than their users do. Consumers show little awareness of advanced data uses such as tracking and targeted advertisements.*

3.2 Do consumers understand?

As set out in the previous section, consumers by and large tend to skip privacy policies. If consumers were to read such policies, however, the question would be whether they could understand them. This question has to be understood as having three different dimensions. First, there is the issue of whether consumers have a correct understanding of what a privacy policy is. Second, there is the issue of whether consumers understand its content. Third, there is the issue of whether consumers understand the consequences of (dis)agreeing with it. This section addresses these three dimensions of consumers' understanding of privacy policies in turn, and it presents the respective insights identified from the relevant literature.

First dimension – Do consumers understand what a privacy policy is?

A study by Feldman et al.[73] in 2005 finds that the majority of Internet users in the USA (59%) are under the impression that the mere existence of a privacy policy on a website means that the website will not share personal data with third parties. Turow et al.[74] confirm this result for Californian consumers. They find that 55% of them hold this

73 Feldman, L.; Turow, J.; Meltzer, K. (2005): Open to Exploitation: American Shoppers Online and Offline. Annenberg Public Policy Center.

74 Turow, J.; Mulligan, D.K. and Hoofnagle, C.J. (2007): Research Report: Consumers Fundamentally Misunderstand the Online Advertising Marketplace. Samuelson Law, Technology, & Public Policy Clinic/Annenberg Public Policy Center.

belief. King and Hoofnagle[75] present similar figures. In a similar vein, studies on online shopping indicate that if a website has got a privacy policy, this fact alone enhances consumers' trust significantly. Consequently, in the presence of a privacy policy, consumers are willing to disclose more personal information;[76] they are more likely to make a purchase;[77] and they show generally higher levels of trust and belief that their data is well protected.[78]

In fact, the term "privacy policy" may be quite misleading as consumers infer that there is a policy in place that protects consumers' privacy;[79] the step taken by Facebook to use the term "Data Use Policy" may be considered a more accurate term.[80] On the other hand, it is quite telling that the term appears to stem from the sphere of market research where, for instance, Nielsen uses it to describe their policy related to the data from their consumer panels. So far, we have not been able to identify any research that explicitly addresses this issue, for instance through explorative research into what terminology consumers actually use when discussing privacy online. It may present a promising avenue to develop terminology that makes privacy policies more accessible to consumers.

A related issue is the privacy beliefs and trust triggered by privacy seals and similar graphic representations. Moores[81] indicates that consumers may be swayed by almost any such label to trust a website's privacy policy. Other studies, however, shed light on the more subtle underlying effects. For instance, Böhme and Köpsell[82] show that changes in parts of the text used for consent dialogues can influence the likelihood of consent significantly. Böhme and Köpsell draw this conclusions based on an experiment with 80,000 users of an online privacy tool. Each user was presented with a consent dialogue of around 200 words length. Consent dialogues varied randomly in

---

75 Hoofnagle, C.J.; King, J. (2008): What Californians Understand about Privacy Online (UC Berkeley). Research Report.

76 Hui, K.L.; Teo, H.H. and Lee, S.Y.T. (2007): The Value of Privacy Assurance: An Exploratory Field Experiment. MIS Quarterly 31: 19-33.

77 Jensen, C.; Potts, C.; Jensen, C. (2005): Privacy Practices of Internet Users: Self-Reports versus Observed Behavior. International Journal of Human-Computer Studies 63: 203-227.; Tsai, J.Y.; Egelman, S.; Cranor, L.; Acquisti, A. (2011): The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. Information Systems Research 22: 254-268.

78 Jensen, C.; Potts, C.; Jensen, C. (2005): Privacy Practices of Internet Users: Self-Reports versus Observed Behavior. International Journal of Human-Computer Studies 63: 203-227.; Li, H.; Sarathy, R.; Xu, H. (2011): The Role of Affect and Cognition on Online Consumers' Decision to Disclose Personal Information to Unfamiliar Online Vendors. Decision Support Systems 51: 434-445.

79 Turow, J.; Hoofnagle; C. J.; Mulligan, D. K.; Good, N.; Grossklags, J. (2007): The Federal Trade Commission and Consumer Privacy in the Coming Decade. A Journal of Law & Policy for the Information Society 3(3) I/S: 723.

80 Beese, J. (2012): Facebook Removes "Privacy" From New Data Use Policy. SproutSocial 23-03-2012. Available at: http://sproutsocial.com/insights/facebook-data-use-policy/. Cf Zuiderveen Borgesius, F. J. (2015): Improving Privacy Protection in the Area of Behavioural Targeting (PhD thesis University of Amsterdam), Kluwer law International (forthcoming).

81 Moores T. (2005): „Do Consumers Understand the Role of Privacy Seals in E-Commerce?" Communications of the ACM 8648(3), 89-90.

82 Böhme, R. and Köpsell, S. (2010): Trained to Accept? CHI '10 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Atlanta, Georgia, USA: 2403-2406.

terms of three parts of the text throughout the experiment: (1) Heading: A polite request for help was compared to a neutral text; (2) Button text: This could resemble a typical EULA using "I accept" and "I decline" as compared to a voluntary option "I take part" and "I do not take part"; and (3) Default option: The default could be set to consent, objection or no default at all. Across 81,920 user responses, Böhme and Köpsell find that dialogues resembling a EULA received significantly higher participation (i.e. consent) rates than a dialogue indicating actual choice. The polite heading had a slightly negative effect on participation levels, whereas the default button could increase participation levels when set to "consent". Their results indicate that consumers who are faced with a dialogue that resembles their expectations in an official graphic are more likely to follow a heuristic processing route and agree with little or any further engagement.

LaRose and Rifon[83] add another important dimension to understanding the effect of privacy warning labels,[84] namely personal involvement[85] and self-efficacy[86] with privacy. In their experimental design, they test the reactions of 227 undergraduate students sorted into high and low privacy involvement groups to a stimulus website featuring either a privacy warning label, a privacy seal,[87] both or none of them. They find that subjects with high privacy involvement are generally more likely to expect negative privacy outcomes than those with low privacy involvement. However, no interaction effect was found with privacy warnings or privacy seals. Privacy warning labels, however, significantly increased expectations of negative privacy outcomes. Largely similar effects were found for trust. When a privacy seal was also present, this effect was reduced.

As regards behavioural outcomes, it was found that privacy seals could increase the willingness to share personal information while a privacy warning label reduced it. The latter effect was not found for subjects with high self-efficacy. It should also be noted that privacy seals only increased the willingness to disclose personal information in subjects with high privacy involvement when their self-efficacy was relatively low. Among those with low privacy involvement, however, the opposite effect was found, i.e. seals led to an increase in disclosure for those with low privacy involvement, but had no effect on subjects with high self-efficacy. Privacy warning labels also reduced the

83 LaRose, R. and Rifon, N.J. (2007): Promoting i-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior. The Journal of Consumer Affairs 41(1): 127-149.

84 Privacy warning labels were built from the actual information on the privacy policy of amazon.com by condensing the information into clear and succinct messages summarising the privacy risks and benefits to consumers. The specific warning label used is reproduced in LaRose and Rifon's paper.

85 Privacy involvement is a measure to describe the personal relevance of privacy to an individual consumers. LaRose and Rifon (2007) used a four-item semantic scale to measure this construct. Privacy […] (1) matters to me; doesn't matter to me; (2) is of no concern to me, is of concern to me; (3) is irrelevant, is relevant to me; (4) is important, is not important to me.

86 Self-efficacy is used by LaRose and Rifon (2007) to measure an individual's perceived ability to protect their privacy on the Internet. They used a ten-item scale consisting of seven-point Likert-type items to measure it. Further details on these items and the scale can be found in in their paper.

87 The widely known TRUSTe seal was used for this purpose. It can be found at http://www.truste.com.

buying intentions of the subjects. These results indicate that it may actually be the two most vulnerable groups of consumers who are most likely swayed to disclose personal data using privacy seals. First, there are the consumers who are more concerned about online privacy than the average consumer, but who do not have the skills to protect themselves. Second, there are the consumers who have such skills but do not care about privacy.

Second dimension – Do consumers understand the content of privacy policies?

There is broad consensus in the literature that privacy policies are cumbersome, poorly written and difficult to understand mainly due to the legalistic jargon they use. As shown in a recent Eurobarometer survey,[88] around 25% of Europeans have difficulty reading data protection policies.[89] In fact, this is probably a vast underestimation of the actual magnitude of the issue, as most strikingly, a study conducted by Hoofnagle and King[90] reports that even law students have significant problems understanding privacy policies. In addition to their complexity, vagueness of terminology may also impede consumers' understanding of privacy policies.[91]

Broader insights can be gained from analysing privacy policies using so-called readability score systems. There are various kinds of such tests.[92] Commonly, they provide a readability score based on the length of the text, the length of individual words, the number of syllables per word and similar characteristics. The respective score corresponds with a specific level of reading likely to be attained through formal education. Cadogan[93] exemplifies this with an in-depth analysis of three selected privacy policies (PrivacyAlliance.org; Dell.com and Amazon.com). She finds that all three privacy policies require a high level of reading competence. Rowan and Dehlinger's[94] study analyses the readability of privacy policies of mobile health and fitness applications, which represents a particularly sensitive field regarding privacy of personal data. They found that the reading grade averages across the readability measures for most applications tested require reading ability above the 12th (US) grade

88 European Commission, "Special Eurobarometer 359: Attitudes on data protection and electronic identity in the European Union" (2011) http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf, p 112-114.

89 In light of the study by Hoofnagle and King (2007), this figure appears to be relatively low. Again, we are likely facing a strong bias in consumers' self-reports as not many consumers would like to admit to having difficulty understanding such policies.

90 Hoofnagle, C.J. and King, J. (2007): Consumer Information Sharing: Where the Sun Still Don't Shine. University of California, Berkeley.

91 Good, N.; Grossklags, J., Thaw, D.; Perzanowski, A.; Mulligan, D. K.; Konstan, J. (2006): User Choices and Regret: Understanding Users' Decision Process about Consensually Acquired Spyware. A Journal Of Law And Policy For The Information Society, Issue (2006), 323.

92 For an example see Massey, A. K.; Eisenstein, J.; Anton, A. I., Swire, P.P. (2013): Automated Text Mining for Requirements Analysis of Policy Documents. Requirements Engineering Conference (RE), 2013 21st IEEE International: 4-13.

93 Cadogan, R.A. (2004): An Imbalance of Power: The Readability of Internet Privacy Policies. Journal of Business and Economic Research 2(3): 49-62.

94 Rowan, M. and Dehlinger, J. (2014): A privacy policy comparison of health and fitness related mobile applications. Procedia Computer Science 37(2014): 348-355.

level. In a similar study, Ermakova et al.[95] confirmed that current privacy policies are difficult to read for consumers. Their analysis involved the privacy policies of 5,431 healthcare websites, which they compared to those found on 1,166 e-commerce websites. They found healthcare websites' privacy policies on average to be more readable for users than those offered by e-commerce websites.

In a prototype of a financial privacy notice, six meta requirements to increase understanding were pointed out:[96]

1. Keep it simple
2. Good design matters
3. Careful design decisions ensure neutrality
4. A "whole-to-part" design is critical to comprehension
5. Standardization is highly effective
6. The disclosure table is critical

These requirements seem indisputable, but based on the results by McDonald et al.,[97] it may be debated whether readability is really the most relevant issue to be addressed. Their results indicate that readability may actually not be a good predictor for the performance of privacy policies when it comes to informing consumers. We describe and discuss this study in section 4.1 of this report.

Third dimension – Do consumers understand the consequences of their actions?

The third facet of understanding refers to whether consumers can actually grasp what their (dis)agreement with privacy policies entails.

First and foremost, the complexity of the continuously evolving system of data flows mediated by data aggregators, ad networks, ad exchanges and third-party tracking companies among others renders it virtually impossible to fathom the full scope of what may or may not happen with one's personal data.[98] Thus, the information asymmetry between the provider of a website, service or product and the consumer is likely to persist even despite a privacy policy that is per se easy to understand. In fact, this hints

95 Ermakova, T.; Fabian, B. and Babina, El (2015): Readability of Privacy Policies of Healthcare Websites. Thomas, O. and Teuteberg, F. (Eds.): Proceedings der 12. Internationalen Tagung Wirtschaftsinformatik (WI 2015). Osnabrück: 1085-1099.

96 Kleimann Communication Group (2006): Evolution of a Prototype Financial Privacy Notice. A Report con the Form Development Project. Similar requirements are summarised in a publication by the German consumers association Verbraucherzentrale Bundesverband (vzbv) (2011): Information gut, alles gut? Berlin.

97 McDonald, A.M.; Reeder, R.W.; Kelley, P.G. and Cranor, L.F. (2009): A Comparative Study of Online Privacy Policies and Formats. Privacy Enhancing Technologies – Lecture Notes in Computer Science 5672: 37-55.

98 Barocas, S. and Nissenbaum, H. (2009): On Notice: The Trouble with Notice and Consent. Proceedings of the Engaging Data Forum. The First International Forum on the Application and Management of Personal Electronic Information; Acquisti A.; Grossklags J. (2007): What Can Behavioral Economics Teach Us About Privacy?, in Acquisti A et al. (eds), Digital Privacy: Theory, Technologies and Practices. Auerbach Publications, Taylor and Francis Group.

at the so-called transparency paradox, a term coined by Nissenbaum.[99] It captures the idea that "transparency of textual meaning and transparency of practice conflict in all but rare instances".[100] This means that for a privacy policy to be actually transparent, the policy needs to be detailed and point out exactly who interacts with the data, when, how and to what end. However, this detail renders the texts so complex that no one reads them, let alone understands them. Furthermore, even if consumers were to be able to comprehend who has access to their personal data, what is happening to it and for what purposes, the problem of predicting the actual consequences persists.[101] For instance, it is impossible to predict the specific consequences of a data security breach as even large (and presumably trustworthy) companies have been subject to successful hacker attacks. Equally, it is difficult for a consumer to predict whether any other potentially adverse effect such as price discrimination are likely to occur at the individual level.

However, the actual possibility of such adverse effects of consumer profiling rests largely on the accuracy of profiling systems. A recent study by Rao et al.,[102] however, disputes this accuracy. They make use of the possibility that consumers may gain access to their personal profiles on data aggregators[103] and discuss individuals' profiles with them in depth (n=8 in-depth interviews). They further validate their results using an online survey (n=100) that asks consumers to check their profiles themselves and provide insights as to how accurate they are as well as their level of concern about the fact that this data is collected and put to use. Rao et al. find that consumer profiles were inaccurate for 8 out of 8 participants in the in-depth interviews and 45% of the survey respondents. Besides shedding some doubts on the practice of targeted advertising itself, they emphasise that this also violates the data quality principle.[104] On the other hand, it should be noted that Castelluccia et al.[105] show that one can reconstruct the Google interest profiles of consumers based on the advertisement data and vice versa.[106] However, they only aim to reconstruct what is there and do not check if the profiles are an actual representation of the individual consumer.

Behavioural sciences have pointed to various cognitive biases that either may sway consumers to consent without considering the consequences much at all or may

---

99 Nissenbaum, H. (2011): A Contextual Approach in Privacy Online. Daedalus 140(4): 32-48.

100 Ibid. 36.

101 Zuiderveen Borgesius, F. J. (2015): Improving Privacy Protection in the Area of Behavioural Targeting (PhD thesis University of Amsterdam), Kluwer law International (forthcoming).

102 Rao, A.; Schaub, F. and Sadeh, N. (2014): What do they know about me? Contents and Concerns of Online Behavioral Profiles. 2014 ASE BigData/SocialInformatics/PASSAT/BioMedCom 2014 Conference, Harvard University, December 14-16, 2014.

103 Rao et al. name BlueKai, Google, Yahoo, Acxiom and Microsoft as examples.

104 This is the second OECD Privacy Principle, see http://oecdprivacy.org/#quality

105 Castelluccia, C.; Kaafar, M.A.; Tran, M.-D. (2012): Betrayed by Your Ads! Reconstructing User Profiles From Targeted Ads. Privacy Enhancing Technologies – Lecture Notes in Computer Science Vol. 7384: 1-17.

106 Datta, A.; Tschantz, M. C.; Datta, A. (2014): Automated Experiments on Ad Privacy Settings: A Tale of Opacity, Choice, and Discrimination. Proceedings of Privacy Enhancing Technologies Symposium, July 2014.

impede consumers from grasping the consequences of (dis)agreeing with terms and conditions. For instance, in section 3.1, the *status quo bias* has already been discussed. It refers to consumers' general preference for default options found in numerous fields, for example organ donation legislation, which in turn also makes them inclined to opt for the default options for privacy settings. The so-called framing effect may further enforce consumers' tendency to quick and easy choices, as Högberg's experiment illustrates.[107] Högberg shows that a framing effect occurs when consumers are faced with the decision to use manual control for the information settings or a quick default option when entering into a cloud service. In total, he assigned 121 subjects randomly to three conditions: (1) a framing text that emphasised the time one could save by simply opting for quick default settings; (2) a framing text that emphasised the control that one would have over one's data when s/he chose the manual setting option; or (3) no framing. When shown the first framing, more than half of the subjects opted for the quick default settings. In the second condition, however, more than 80% opted for the manual setting procedure. With no framing, fewer subjects opted for the manual path (77%).

Similar to framing, the halo effect refers to consumers' tendency to judge all traits of a given subject based on a specific trait they are familiar with. This kind of "spillover" from one trait to others has been documented with relevance to privacy policies by Orito et al.[108] In their survey of 597 "millennials" in Japan, they find that an established positive image of online shopping sites has a greater impact on their perceived trustworthiness than privacy seals.

While these first types of cognitive biases may incline consumers to simply consent to privacy policies without deliberating the consequences much, there are also cognitive biases that impede them from understanding the consequences of consenting, for example because they underestimate them. First, *hyperbolic discounting* is worth mentioning. It describes the effect that humans commonly prefer instant gratification over long-term benefits. Acquisti and Grossklags[109] recognise consumers' tendency to hyperbolic discounting in a 2002 Jupiter Research survey, in which 82% of respondents would have been willing to disclose personal data to a shopping website that they had not yet made a purchase on in exchange for a US$100 sweepstake entry. Such behaviour may be further supported by the illusion of control over one's data. As we will show in the following section (3.3), consumers in fact have very little if any control over who collects their personal data when they are online and what happens with their data once it has been collected. In their exploratory survey of 260 Irish respondents, Doherty

107 Högberg, J. (2013): The effect of effort, control and value frames on online users privacy decision. Master's Thesis at the Faculty of Economic Sciences, Communication and IT. Karlstad University.

108 Orito, Y.; Murata, K. and Fukuta, Y. (2013): Do online privacy policies and seals affect corporate trustworthiness and reputation? International Review of Information Ethics 19(7): 52- 65.

109 Acquisti, A. and Grossklags, J. (2004): Privacy Attitudes and Privacy Behavior. Gains, Losses and Hyperbolic Discounting. In Camp, J. and Lewis, R. (Eds.): The Economic of Information Security. Berlin, Kluwer.

and Lang[110] find indications for the illusion of control. In their sample, there is a positive correlation between perceived control over one's personal data and the willingness to disclose this data, i.e. respondents with a higher level of perceived control are willing to disclose more personal data. This happens despite the fact that the actual level of control over one's data is probably very similar across respondents.

While all these biases may be employed to consumers' disadvantage, they also open avenues to improve the likelihood of consumers engaging with privacy policies (i.e. read them), understanding them and acting accordingly. We discuss some corresponding approaches in chapter 4.

Do consumers understand?

- *Consumers commonly show misconceptions of privacy policies. In the presence of a privacy policy, consumers are willing to disclose more personal information; they are more likely to make a purchase; and they show generally higher levels of trust and belief that their data is well protected.*
- *Even law students were found to have significant problems understanding privacy policies. Privacy policies tend to be cumbersome, poorly written and difficult to understand mainly due to the legalistic jargon they use.*
- *It is difficult if not impossible for consumers to understand the consequences with respect to personal data processing. This is likely to be due to information asymmetry being fostered by the complexity of the continuously evolving system of data flows mediated by data aggregators, ad networks, ad exchanges and third-party tracking companies.*

3.3 Do consumers act after reading?

To approach this third question, it is first of all necessary to understand consumers' actual scope to act. Their scope to act, for instance to avoid tracking and potential personal data breaches, appears very limited for various reasons. This section starts by exploring these reasons in order to set the scene before describing the actions that consumers may take.

110 Doherty, C. and Lang, M. (2014): An Exploratory Survey of the Effects of Perceived Control and Perceived Risk on Information Privacy. 9th ANNUAL SYMPOSIUM ON INFORMATION ASSURANCE (ASIA'14), JUNE 3-4, 2014, ALBANY, NY: 23-28.

The first reason that is often cited in the literature on online privacy is the so-called "take it or leave it" policy[111] currently in use on the majority of websites, applications, services and products. A consumer can either accept a privacy policy and use the respective website, application, service or product, or if s/he declines the policy, s/he is unable to use it. This implies that there is no real choice. Interestingly, when asked about their reaction to this practice, 68% of Canadians claim to have chosen not to use a website because of discomfort over privacy terms.[112] This number is surprising in light of the insights presented in sections 3.1 and 3.2, which clearly illustrate that the vast majority of consumers do not read or understand the privacy policies of websites. On the other hand, one may attribute this finding to the halo effect (described in 3.2), which may lead consumers to mistrust a website's privacy policy not because they read it, but because other characteristics of the website trigger mistrust.

In some cases, consumers may be swayed to opt in to privacy policies within a "take it or leave it" regime due to network effects even if they disfavour parts or the whole privacy policy. For instance, if all your friends have joined a specific social network, you have little to gain from joining another possibly more privacy-friendly one.[113] In line with Wauters et al.'s argument, as soon as a consumer has joined a SNS and is profiting from network effects, lock-in effects may come into play. Even if s/he then finds that s/he disagrees with the current privacy policy or a change in the privacy policy of the SNS, s/he might still not leave the SNS. Another example of such lock-in effects is the transfer of all one's data from one provider to another, which incurs significant switching costs for the user.[114] In the end, they may stick to a web service or application despite their disagreement with its privacy policy.

The evolution of tracking technology further limits consumers' scope for action. In fact, data harvesting may commence as soon as a browser opens a website, or if Deep Packet Inspection[115] (DPI) is used, even as soon as a consumer's device gains access to the Internet. In contrast, however, privacy policies can only be accessed (i.e. read, understood and potentially consented to) when the consumer is already on the respective website.

---

111 Nissenbaum, H. (2011): A Contextual Approach to Privacy Online. Daedalus 140(4): 32-48.; Wagenaar, R.W. and Eldin A.M.T. (2003): Towards a Component Based Privacy Protector Architecture. Proceedings 15th Conference On Advanced Information Systems Engineering – Klagenfurt, Oostenrijk: 1-11.

112 Phoenix Strategic Perspectives (2013): Survey of Canadians on Privacy-Related Issues. Prepared for the Office of the Privacy Commissioner of Canada.

113 Wauters, E.; Lievens, E. and Valcke, P. (2013): D1.2.4: A legal analysis of Terms of Use of Social Networking Sites, including a practical legal guide for users: 'Rights & obligations in a social media environment. iMinds-ICRI – KU Leuven. And Zuiderveen Borgesius, F. J. (2015): Improving Privacy Protection in the Area of Behavioural Targeting (PhD thesis University of Amsterdam), Kluwer law International (forthcoming).

114 Shapiro, C.; Varian, H.R. (1999): Information Rules. A Strategic Guide to the Network Economy. Harvard Business School Press, p 104.

115 For an explanation see Glossary section.

Tracking technology has moved beyond this point already. Device fingerprinting enables the unique identification of a broad range of devices. These devices can then be tracked and the resulting data can be used to build profiles about the consumers using their devices. Such profiles can therefore be extended by using data from offline third parties. While this technology can be used to the benefit of web users, for instance by preventing identity theft or credit card fraud, it also means consumers can be tracked across all their devices. As this does not require the installation of cookies or otherwise interfering with the devices as such, consumers have virtually no chance of evading this practice.[116]

Device fingerprinting refers to various techniques that identify devices connected to the Internet based on information about a device's configuration and the features it supports. As the device-specific combination of applicable configurations and features typically offers sufficient entropy, meaning the information varies from one device to another, it qualifies as a device-specific fingerprint.

In a large-scale experiment looking at web browser configurations, Eckersley found more than 18 bits of entropy, which means "that if we pick a browser at random, at best we expect that only one in 286,777 other browsers will share its fingerprint".[117] If a browser supported Flash or Java, Eckersley was able to uniquely identify 94.2% of browsers. The study also considered fingerprints to change over time, which would challenge a website operator's ability to identify returning devices. This could be solved by incorporating a simple heuristic resulting in 99.1% of guesses of updated fingerprints being correct, which means that even if fingerprints change over time, it will be relatively easy for websites to uniquely identify returning devices with high accuracy.

Mowery and Shacham[118] focused on device fingerprinting using the canvas element,[119] which is supported in modern web browsers as part of the HTML5 standard. They find that a canvas-based fingerprint satisfies multiple "desirable properties". It not only works consistently and has a high entropy, but it is also "orthogonal to other fingerprints", runs "transparent to the user", and is "readily obtainable". The last property means very low hurdles for a website operator. Adding a few lines of JavaScript code to a website is all that it needs to fingerprint devices that are accessing the site. Transparency to the user means that "[t]here is no indication, visual or otherwise, that the user's system is being fingerprinted"[120].

---

116 Rich, J. (2015): Beyond Cookies: Privacy Lessons for Online Advertising. AdExchanger Industry Preview 01-21-2015, available at: https://www.ftc.gov/system/files/documents/public_statements/620061/150121beyondcookies.pdf.

117 Eckersley, P. (2010): How Unique Is Your Web Browser? Privacy Enhancing Technologies. Lecture Notes in Computer Science, Volume 6205: 1-18.

118 Mowery, K.; Shacham, H. (2012): Pixel Perfect: Fingerprinting Canvas in HTML5. Proceedings of Web 2.0 Security & Privacy (W2SP) 2012. IEEE Computer Society: 1-12.

119 See Glossary section.

120 Ibid.

This exemplifies the potential impact on consumers exposed to device fingerprinting. The European Union's Article 29 Data Protection Working Party (WP29) went as far as to summarise that "[d]evice fingerprinting presents serious data protection concerns for individuals".[121] It is interesting to note that WP29 qualifies device fingerprints as personal data. Mowery et al.[122] take a balanced stance in differentiating constructive from destructive uses of device fingerprints. Device fingerprints may, for instance, be used constructively as an anti-fraud mechanism complementing password-based user authentication. By contrast, device fingerprints may, for instance, be used destructively in order to track users across different websites without their knowledge – and thus without their consent.

The study by Nikiforakis et al.[123] provides a strong indication that destructive use of device fingerprinting is the more common case, at least with respect to device fingerprinting for commercial purposes. Their analysis of 3,804 identified websites which use device fingerprinting gives rise to serious doubts about the technique's legitimacy. A total of 1,063 (27.9%) websites found to use device fingerprinting were categorised as "spam" websites. The second most frequent website category to implement device fingerprinting was "malicious sites" (163 cases).

Acar et al.[124] show that fingerprinting practices are used by over 5% of the top 100,000 websites. Compared to evercookies[125] and cookie-syncing[126], they find that canvas fingerprinting is much more widespread. In total, 5.5% of the 100,000 websites use it. They detect 20 canvas fingerprinting domains, out of which 11 belonged to third parties. It should be noted that in their web crawl only homepages were analysed and a deeper analysis may result in finding more canvas fingerprinting activities. Apart from using the Tor Browser,[127] the authors were not able to identify any means that will effectively evade canvas fingerprinting when accessing the Internet. It should be noted that although some websites gave users an option to opt out of canvas fingerprinting, the authors found that the sites were still doing this even after opting out.

121 Article 29 Data Protection Working Party (2014): Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting. 14/EN WP 224: 1-11.
122 Mowery, K.; Bogenreif, D.; Yilek, S.; Shacham, H. (2011): Fingerprinting information in JavaScript implementations. Proceedings of Web 2.0 Security & Privacy (W2SP) 2011. IEEE Computer Society: 1-11.
123 Nikiforakis, N.; Kapravelos, A.; Joosen, W.; Kruegel, C.; Piessens, F.; Vigna, G. (2013): Cookieless Monster: Exploring the Ecosystem of Web-based Device Fingerprinting. 2013 IEEE Symposium on Security and Privacy: 1-15.
124 Acar, G.; Eubank, C.; Engelhardt, S.; Juarez, M.; Narayanan, A. and Diaz, C. (2014): The Web never forgets: Persistent tracking mechanisms in the wild. Proceedings of CCS 2014, Nov. 2014.
125 See Glossary section.
126 See Glossary section.
127 See Glossary section.

Another sophisticated and difficult-to-evade way of identifying the individual user is to analyse the keystroke dynamics. This is almost as precise as a fingerprint.[128] This technology can even be used to analyse the current emotional state of the user.[129]

Given the sophistication of tracking technology, it may be difficult for consumers to successfully evade tracking and targeted advertising. However, as we have briefly highlighted in section 3.1, consumers have found ways to evade targeted advertising in SNS environments. Fransen et al.[130] have recently developed a typology of consumer strategies to resist advertising. They bring together insights over the past 30 years from various strands of literature connected to understanding consumers' reactions to advertising, such as advertising research, psychology or communication research. Their typology defines three types of consumer resistance to advertising: (1) avoidance; (2) contesting; and (3) empowering.

Avoidance of advertising is a well-studied phenomenon. Speck and Elliot's[131] study identifies three kinds of advertising avoidance that still bear significance for consumer behaviour today: (1) physical avoidance; (2) mechanical avoidance; and (3) cognitive avoidance. Physical avoidance describes behaviours that avoid seeing or hearing advertisements. For instance, Drèze and Hussherr[132] document in their study using eye-tracking technology that consumers actively avoid looking at banner advertisements when surfing the Internet. Mechanical avoidance in the case of (targeted) online advertising refers predominantly to using ad blockers[133] that enable consumers to block out some or all of the online advertisements they would otherwise receive. Cognitive avoidance refers to consumers' selective attention. Rejón-Guardia et al.[134] show in a survey of 262 respondents that advertisements' (perceived) offensiveness is positively correlated with cognitive avoidance by consumers. In their study, offensiveness is a second-order construct built from advertisements' perceived clutter, intrusiveness and irritation.

Contesting as a way of consumer resistance to advertisements describes behaviours that actively refute advertisements' (1) content, (2) source or (3) persuasive tactics. The

128 Saevanee, H. and Bhattarakosol, P. (2009): Authenticating User Using Keystroke Dynamics and Finger Pressure. Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE. Keystroke dynamics software is commercially available for biometric authentication since several years and already used to detect e.g. password sharing or license frauds.

129 Epp, C.; Lippold, M. and Mandryk, R.L. (2011): Identifying emotional states using keystroke dynamics. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems: 715-724.

130 Fransen, M.L.; Verlegh, P.W.J.; Kirmani, A. and Smit, E.G. (2015): A typology of consumer strategies for resisting advertising, and a review of mechanisms for countering them. International Journal of Advertising 34(1): 6-16.

131 Speck, P.S. and Elliot, M. (1997): Predictors of advertising avoidance in print and broadcast media. Journal of Advertising 26(3): 61-76.

132 Drèse, X. and Hussherr, F.-X. (2003): Internet advertising: Is anybody watching? Journal of Interactive Advertising 17(4): 8-23.

133 For example: AdBlock Plus (www.adblockplus.org) and BluHell (addons.mozilla.org).

134 Rejón-Guardia, F.; Sánchez-Fernández, J.; and Muñoz-Leiva, F. (2014): A Generalization of Advertising Avoidance Model on Social Network. Working Paper in Review.

first kind of contesting behaviour was established early on in persuasion research.[135] It describes consumers' engagement in counter-arguing the content of advertisements trying to refute them logically. While one may assume that this behaviour does not differ between traditional and online advertising environments, the other two kinds of contesting behaviour appear to bear more significance for the present study. Contesting the source of an advertisement refers to consumers' dismissal of the credibility, trustworthiness or expertise of the source.[136] Generally, word-of-mouth marketing, for example recommendations by trustworthy friends (possibly induced by advertising), has been consistently shown to lead to the least source contesting.[137] This raises the question of how consumers react to recommendations by friends on SNSs, some of which are in fact paid-for advertisements although, for example, they still reflect actual "Likes" by Facebook friends. To the best knowledge of the authors of this report, to date there is only indicative evidence on consumers' reactions to this specific kind of targeted advertisements. For instance, a recent IAB (Interactive Advertising Bureau) article[138] indicates that only about one-fifth of SNS users rate such recommendations as influential for their purchase decisions. In a similar vein, it is as yet unclear how consumers' awareness of persuasive tactics used by targeted online advertising actors affects their contesting behaviour on SNSs, for example.

The third type of consumers' advertising resistance identified by Fransen et al. is empowering strategies. Again, there are three strategies available to consumers: (1) attitude bolstering, (2) social validation and (3) self-assertion. Consumers engage in attitude bolstering by actively avoiding a message's content that refutes their own opinion. Instead, they focus on thoughts and arguments they are familiar with to support their own position.[139] Social validation is used by consumers to get social proof of their existing attitudes if a persuasive message seeks to counter them.[140] Self-assertion was identified by Jacks and Cameron as consumers reminding themselves about being confident about their own attitudes.[141] Again, the latter two strategies merit further research within the field of targeted advertising employing personal data and interaction with "friends" on SNSs. For instance, it would be relevant to understand if and how the messages that individual consumers see in their timelines may influence their social validation and self-assertion practices.

---

135 e.g. Buller, D.B. (1986): Distraction during persuasive communication: A meta-analytic review. Communication Monographs 53: 91-114.

136 e.g. Jacks, J.Z. and Cameron, K.A. (2003): Strategies for resisting persuasion. Basic and Applied Social Psychology 25(2): 145-161.

137 e.g. Godes, D. and Mayzlin, D. (2004): Using online conversations to study wor-of-mouth communication. Marketing Science 23(4): 545-560.

138 IAB (2014): Facebook fails on advertising front but scores as branding platform, says iLead. Available at: http://iabsa.net/research-data/facebook-fails-on-the-advertising-front-but-scores-points-as-branding-platform-ilead/.

139 e.g. Meirick, P. (2002): Cognitive responses to negative and comparative political advertising. Journal of Advertising 31(1): 49-62.

140 Jacks, J.Z. and Cameron, K.A. (2003): Strategies for resisting persuasion. Basic and Applied Social Psychology 25(2): 145-161.

141 Ibid.

Finally, consumers are confronted with great uncertainty as regards if, how much and to what end their personal data is gathered and further used when they visit a website or consume a digital service or product (see section 3.2). Only the provider of the website, service or product can possibly know about this. This information asymmetry also impedes a market for personal data, in which consumers could either invest more time into managing their privacy or would be willing to pay for it.[142] In other words, the problem of quality uncertainty is an implicit characteristic of web services, and the situation suggests that the market for privacy-friendly websites or applications has characteristics of a lemons market i.e. where there is a market failure as a result of information asymmetries.[143] Consequently, it is not surprising that only very few websites position privacy protection as their competitive advantage.[144] After interviewing consumers in the online marketing business, Turow concludes that competition pushes firms towards privacy-invasive marketing practices, which further confirms the "lemons market" situation.[145]

Do consumers act after reading?

- *Consumers' scope to act, for instance to avoid tracking and potential personal data breaches, appears very limited. This is mainly due to the widespread use of "take it or leave it" privacy policy regimes, network and lock-in effects and the evolution of difficult-to-evade tracking technology such as device fingerprinting.*
- *Consumers are confronted with great uncertainty as regards personal data uses when they visit a website or consume a digital service or product. This information asymmetry impedes a market for personal data, in which consumers could either invest more time into managing their privacy or would be willing to pay for it.*
- *Consumers have developed strategies to resist advertising, including avoidance, contesting and empowering strategies.*

142 Strandburg, K. J. (2013): Free Fall: the Online Market's Consumer Preference Disconnect. New York University Law and Economics Working Papers. Paper 354, p 156.

143 Vila, T.; Greenstadt, R.; Molnar, D. (2004): Why We Can't be Bothered to Read Privacy Policies. Models of Privacy Economics as a Lemons Market. Proceeding ICEC '03 Proceedings of the 5th international conference on Electronic commerce: 403-407. Zuiderveen Borgesius, F. J. (2015): Improving Privacy Protection in the Area of Behavioural Targeting (PhD thesis University of Amsterdam), Kluwer law International (forthcoming). We explain the term "lemons market" in the Glossary section.

144 For instance, two search engines position themselves as not collecting the personal data of their users: www.duckduckgo.com and www.startpage.com .

145 Turow, J. (2011): The Daily You: How the New Advertising Industry is Defining Your Identity and Your Worth. Yale University Press 2011, p 199. Cf Zuiderveen Borgesius, F. J. (2015): Improving Privacy Protection in the Area of Behavioural Targeting (PhD thesis University of Amsterdam), Kluwer law International (forthcoming).

4 Potential to improve informed consent in practice

4.1 How to improve readership?

The preceding chapter has clearly shown that there is little if any consumer engagement with terms and conditions they agree to. In theory, reducing the cost of reading for consumers to a level that equals the benefit that they receive from reading it ought to suffice to solve the problem of readership. In practice, however, problems arise. First, as we have shown in section 3.1, consumers spend little time engaging with most online content – and even if they did, the cost of reading (in time spent reading) is likely too significant and is unlikely to fall. Second, the benefit of reading terms and conditions is unclear to consumers. Therefore, its economic value is also difficult to establish. Third, insights from behavioural economics illustrate clearly that consumers are unlikely to act rationally. In sum, this raises the question of if and how consumers are likely to engage with terms and conditions.

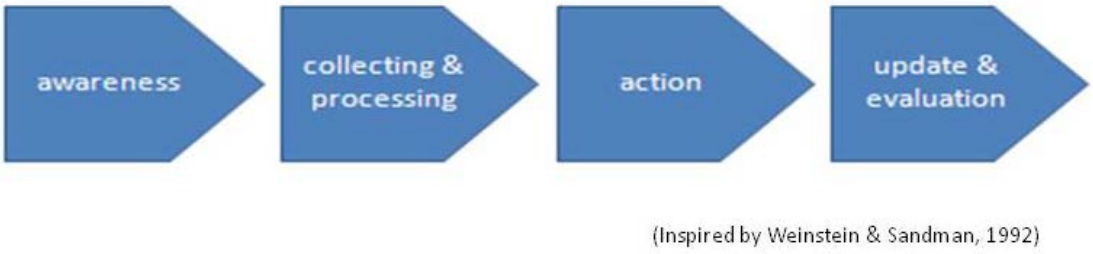
To address the question, an approach from the realm of advertising effectiveness research may prove useful. Originally developed to understand attitude change due to persuasive messages, the Elaboration Likelihood Model (ELM) by Petty and Cacioppo[146] can provide a framework to study how to improve likelihood of consumers engaging with the terms and conditions they agree to. The model predicts that the persuasive effect of stimuli depends on the subject's motivation and ability to devote cognitive effort to processing the respective stimuli. Under conditions of high motivation and/or high ability, subjects are likely to follow the so-called central route of information processing. Under these conditions, consumers are more likely to engage with quality arguments even if they require extensive cognitive engagement. When motivation and/or ability are low, however, subjects are likely to follow the so-called peripheral route of information processing. Under these conditions, consumers are more likely to engage with easy to process and often heuristic cues. This theory thus integrates the likelihood of reading as such and the likelihood of understanding the message. We discuss the studies that provide indications for how to address the first part in this section and studies addressing the second part in the following section to reflect the structure of the preceding chapter of this report.

While this widely accepted model does not provide a direct answer to the issue of readership of terms and conditions, it points clearly to the relevant points that need to be addressed. Elevating motivation in consumers to engage with terms and conditions is likely to move them to a central route of information processing. Studies addressing this point are scarce.

146 Cacioppo, J. T.; Petty, R. E. (1983): Social psychophysiology: A sourcebook. New York: Guildford Press.

Helberger[147] is one of the few researchers, who argue in a similar way when she points out that a key to understanding the terms and conditions for the effective communication of consumer information is to realise that consumer information is not a one-off act but a process. For conveyed information to be actually beneficial to consumers, Helberger explains, consumers have to pass a number of steps first: this is termed the behavioural information pathway.[148]

Figure 4-1: The behavioural information pathway



Source: Helberger, N. (2013)

The behavioural information pathway covers several steps mentioned above (see Figure 4-1): consumers first have to become aware of the importance of information on privacy so that they engage with the topic and understand what data collecting and processing activities mean. This enables them to act upon information.

Raising awareness and in turn elaboration likelihood requires an understanding of the consequences of the use of personal data by, for example, online behavioural advertising and raising awareness of its effects.[149]

As indicated by studies that highlight the relevance of contextualisation in section 4.2, measures to raise consumers' awareness of potential consequences of their consent are likely to be most effective in situ i.e. when they are visiting a particular website or using a specific application. Modern website technology enables creating new display formats and menu navigations by using responsive web design. For instance, companies like Facebook or online shops like Amazon and eBay use new options for presenting information, i.e. videos or click-through menus. The method of downloading

147 Helberger, N. (2013): Form Matters: Informing Consumers Effectively. Amsterdam Law School Research Paper No. 2013-71/Institute for Information Law Research Paper No. 2013-10.

148 Helberger, N. (2013): Form Matters: Informing Consumers Effectively. Amsterdam Law School Research Paper No. 2013-71/Institute for Information Law Research Paper No. 2013-10: 9.

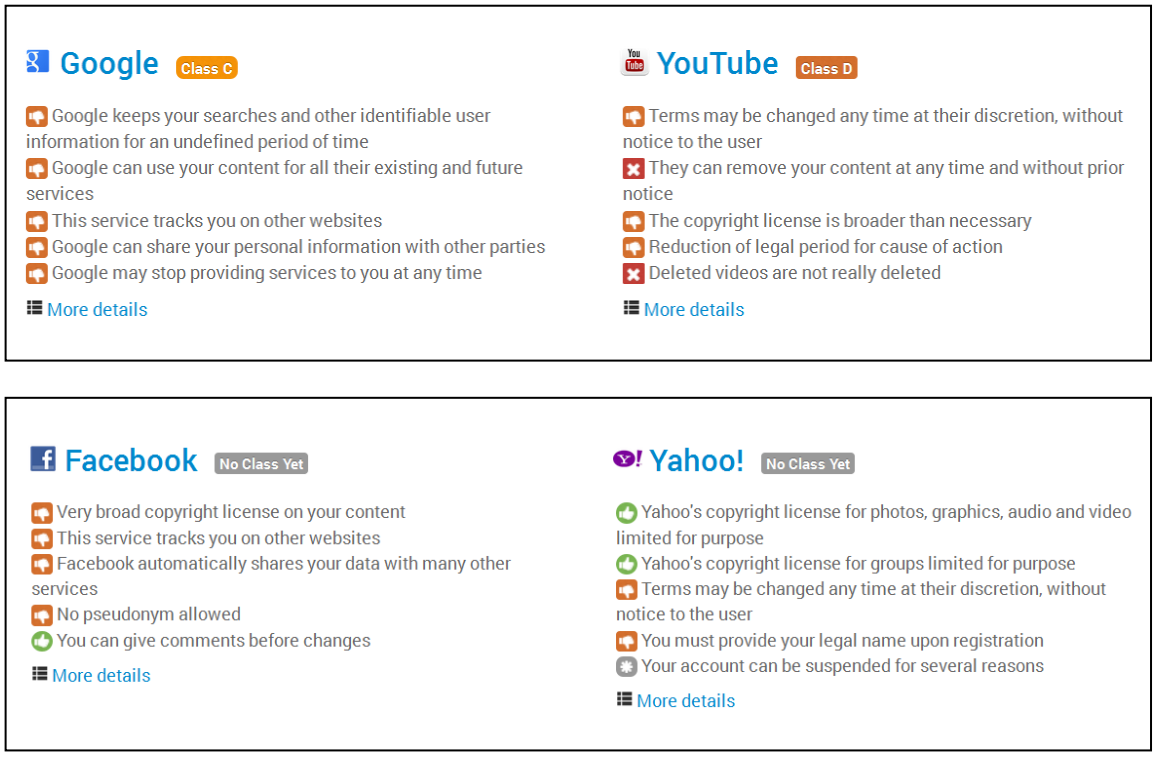
149 Aïmeur, E.; Brassard, G.; Rioux, J. (2013): Data Privacy: An End-User Perspective. International Journal of Computer Networks and Communications Security. VOL.1, NO.6, November 2013, 237–250.

files in PDF format with long text information is vanishing as new areas of designs for websites are evolving.

There are also a number of user-based initiatives that provide technical support and nudge consumers to the terms of service of the website they currently visit automatically. For instance, the website Terms Of Service Didn't Read (tosdr.org) offers a browser add-on that provides easy-to-understand feedback to consumers about the quality of the terms of service they most likely have not read. The project started in 2012 and is funded by donations.[150] Its outcome is based on free software and open data principles which means that anyone can download and use the service for free.

To date, only a few web services like Google or YouTube are rated in a five-class system from Class A ("very good") to Class E ("very bad"). Others like Facebook and Yahoo are registered and described but not rated yet.

Figure 4-2: Examples of "Terms of service didn't read" – tosdr.org



Source: Screenshots from tosdlr.org (22 March 2015)

150 The project goes back to computer programmers ("hackers") who met at the regular international Chaos Communications Camp in Berlin. Topics of the camp are privacy, freedom of information, and data security. The term "tl;dr" means "too long; didn´t read" and is widely used to indicate that texts other users posted are of excessive length.

In sum, awareness of the consequences of consenting to privacy policies may be a key driver of consumers' elaboration likelihood. So far, however, this appears to be an underrepresented field of research in the current debate. Several new information formats set out to address the issue. However, their effectiveness has yet to be tested. While these approaches aim to move consumers to the central processing route as laid out in the ELM, the other obvious choice is to adapt terms and conditions to the peripheral information processing route. This second approach would require them to be significantly easier to read and understand in order to lower the threshold for consumers to engage with them. In fact, numerous researchers have pursued this idea. In the following section, we summarise this stream of literature.

How to improve readership?

- *The effort of reading terms and conditions is likely to remain high for consumers.*
- *Awareness about the consequences of their actions may, however, be an incentive to engage with terms and conditions.*
- *Several technical solutions are available to make consumers aware of the consequences of their actions in situ.*

4.2 How to improve understanding?

Based on the ELM that has been introduced in the previous section, adapting terms and conditions to the peripheral processing route can improve readership and (in particular) understanding of the message. Consequently, this section presents insights from the literature that indicate how the format, readability or mode of presentation may be improved to make terms and conditions easier to read and comprehend. First, this section describes the relevant experimental research in the area. Second, the section reprises the underlying contradictions that may impede this approach to resolve the problem of reading and understanding terms and conditions. Third, the section looks at approaches that governmental institutions have adopted or recommended.

Experimental approaches to the question whether reading and in particular understanding of terms and conditions can be improved by changes in the presentation and / or format are not scarce.

The studies by studies by Milne and Culnan[151] and Egelman et al.,[152] generally support the correlation between improved readability and enhanced likelihood of reading. Consequently, it is not surprising that numerous researchers have addressed the issue of readability in experimental designs. Research on better ways of presenting privacy policies has been done in several fields like technology design, computer interface design, and psychology.[153] For example, in an experiment with 749 participants McDonald et al.[154] evaluated three formats. First, layered policies, which present a short form with standardised components in addition to a full policy; second, the "Privacy Finder" format, which automatically standardises the text descriptions of privacy practices in a brief bulleted format; and, third, conventional non-standardised human-readable policies. They applied these formats to six real companies' (widely used websites) policies and found out that participants were not able to reliably understand companies' privacy practices in any of the formats. Compared to natural language, respondents read faster with standardised formats, but at the expense of accuracy. The research reveals that all formats and policies were similarly disliked. On the other hand, several studies find a positive effect of readability on consumers' trust.[155]

Besides studying the readability of terms and conditions as such, other approaches have emerged over time that suggest a more drastic change in the presentation of e.g. privacy policies. The most prominent one is to condense legal information related to consumer protection or privacy into icons or labels. In general, these signs visualise requirements of specific certification schemes. While some public administrations act as certification providers, most certification providers are private companies which audit service providers and grant a trust mark.

Similar to food labelling for fair trade or organic products, icons, possibly in conjunction with a trust mark scheme instead of textual representations of terms and conditions,

151 Milne, G.R.; Culnan, M.J. (2004): Strategies for Reducing Online Privacy Risks: Why Consumers Read (or don't Read) Privacy Notices. Journal of Interactive Marketing (18): 15-29.

152 Egelman, S.; Tsai, J.; Cranor, L.F., Acquisti, A. (2009): Timing is Everything? The Effects of Timing and Placement of Online Privacy Indicators. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems: 319-328.

153 See in this context the work of the interdisciplinary research projects SPION (Security and Privacy In Online Social Networks),www.spion.me/publications, and USEMP (User Empowerment for Enhanced Online Management).

154 See McDonald, A.M.; Reeder, R.W.; Kelley, P.G.; Cranor, L.F. (2009): A Comparative Study of Online Privacy Policies and Formats. Privacy Enhancing Technologies, Lecture Notes in Computer Science Volume 5672: 37-55.

155 Milne, G.R. and Culnan, M.J. (2004): Strategies for Reducing Online Privacy Risks: Why Consumers Read (or don't Read) Privacy Notices. Journal of Interactive Marketing 18: 15-29.; Ermakova, T.; Baumann, A.; Fabian, B.; Krasnova, H. (2014): Privacy Policies and Users' Trust: Does Readibility Matter? Proceedings of the Americas Conference on Information Systems (AMCIS, Savannah, USA).; Sultan, F., Urban, G.L.; Shankar, V. and Bart, I.Y. (2002): Determinants and Role of Trust in e-Business. A Large Scale Empirical Study. MIT Sloan School of Management.; Bansal, G.; Zaledi, F. and Gefen, D. (2008): The Moderating Influence of Privacy Concern on the Efficacy of Privacy Assurance Mechanisms for Building Trust: A Multiple-Context Investigation. ICIS Proceedings Paper 7.; Bansal, G.; Zaledi, F. and Gefen, D. (2008): Efficacy of Privacy Assurance Mechanisms in the Context of Disclosing Health Information Online. AMCIS Proceedings. Paper 178.

could significantly facilitate consumers' understanding. They do not have to engage with lengthy terms and conditions, but if they require more information this can be provided, for example by clicking on the trust mark label to open the full terms and conditions agreement. Research indicates, however, that such an approach may be ambiguous. In their study on icons and standard contract terms, Edwards and Abel[156] come to the conclusion that the development of such instruments seems desirable but that it is most effective on an international level because of increasing cross-border e-commerce and worldwide use of social networks that originated in countries outside the European Union's jurisdiction.

Today, there are examples for labelling and certification schemes in the European Union, for example in e-commerce,[157] but their actual use and impact is unclear and has not been examined from a behavioural perspective.[158] More research on the actual effectiveness of privacy icons would be required.[159]

Nevertheless, the European Commission encourages the use of icons,[160] and the European Parliament has proposed making it a requirement for companies to use icons to inform consumers about data-processing practices.[161]

Bashir et al.[162] propose another instrument to condense information and at the same time personalise it to an individual consumer: the Knowledge-based Individualized Privacy Plan (KIPP). KIPP aims to improve consumer comprehension of the significance of privacy notices by personalising information based on different levels of pre-existing knowledge. To underline their hypothesis of diverse consumer background

---

156 Edwards, L.; Abel, W. (2015): The Use of Privacy Icons and Standard Contract Terms for Generating Consumer Trust and Confidence in Digital Services. CREATe Working Paper 2014/15.

157 See for example Trusted Shops for a commercial certification scheme or the EMOTA – European Multi-channel and Online Trade Association label initiative (http://www.euro-label.com). Trust marks have been defined on the European level as: "Electronic labels or visual representations indicating that an e-merchant has demonstrated its conformity to standards regarding, e.g., security, privacy, and business practice." (European Consumer Centres Network - ECC-net (2013): Trust marks report 2013 "Can I trust the trust mark?": 7).

158 For instance, a recent study on the EU-level focuses on the criteria provided by active trust marks to consumers and to collate them, see European Consumer Centres Network - ECC-net (2013): Trust marks report 2013 "Can I trust the trust mark?".

159 For research on a new prototype see e.g. Birrell, E.; Schneider, F. B. (2014): Fine-Grained User Privacy from Avenance Tags. Computing and Information Science Technical Reports. Department of Computer Science, Cornell University.

160 European Commission, Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), COM(2007)228 final, Brussels, 2 May 2007, par 4.3.2. Cf. Zuiderveen Borgesius, F. J. (2015): Improving Privacy Protection in the Area of Behavioural Targeting (PhD thesis University of Amsterdam), Kluwer law International (forthcoming).

161 See Article 13(a), and the annex, of the proposal for a Data Protection Regulation, consolidated version after LIBE Committee vote, 22 October 2013, www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf. Cf. Zuiderveen Borgesius, F. J. (2015): Improving Privacy Protection in the Area of Behavioural Targeting (PhD thesis University of Amsterdam), Kluwer law International (forthcoming).

162 Bashir, M.; Hoff, K.A.; Hayes, C.M.; Kesan, J.P. (2014): Knowledge-based Individualized Privacy Plans (KIPPs): A Potential Tool to Improve the Effectiveness of Privacy Notices, Workshop on the Future of Privacy Notice and Choice, Carnegie Mellon University June 27, 2014.

knowledge, they conducted an online survey among students and found evidence that privacy notices do not usually influence consumer behaviour: only 43% of respondents indicated that they had ever refused to use a website because of privacy policies.[163] In their evaluation of privacy knowledge, 44% of respondents were unaware of the fact that website providers sell user information directly to marketing companies, and 59% did not know that Twitter involves the use of cloud computing. The researchers suggest promoting the understanding of privacy notices by taking into account varying degrees of background knowledge. First, an evaluation process is completed and then the results would be used to form the basis of an individual software-based KIPP profile which would help to interpret privacy notices according to the consumers' pre-settings.

Background knowledge could also involve cultural differences and subsequently these differences would be reflected in national regulations. In an international survey, Bellman et al. focus on possible explanations for differences in Internet privacy concerns reflected in national regulations.[164] By using a sample of Internet users from 38 countries matched against Internet users in the USA, they find support for the need for localised privacy policies.[165] Hence, if website providers would like to make consumers understand (shortened) privacy policies, they should present consumers with privacy policies that take a consumer's cultural background and preferences into account.

In support of the idea that condensed information actually facilitates consumers' understanding, Iyengar and Lepper[166] show that too much information (or choices) can make consumers insecure and unsatisfied. In short, they claim that too many choices mean consumers buy less. A limited choice on the other hand leads to fuller shopping carts. Transferred to a privacy context, this could help understand why consumers tend to ignore data protection settings. We think that they might make consumers feel insecure since they are likely to not understand them fully. Moreover, privacy settings might render consumers dissatisfied as they are supposed to consider all alternative

163 Ibid, p 1. As we have seen before in the findings from Canada, the proportion of users who claim to have chosen not to use a website can be considerably higher (63%) if related to the whole population (see Phoenix Strategic Perspectives (2013): Survey of Canadians on Privacy-Related Issues. Prepared for the Office of the Privacy Commissioner of Canada in chap. 4). An explanation might be that the students in the sample of Bashir et al consider themselves more able to control their handling of personal information or they might be more careless "Internet natives".

164 Bellman, S., Johnson, E.J., Kobrin, S. J., Lohse, G.L. (2004): International Differences in Information Privacy Concerns: A Global Survey of Consumers, The Information Society, 20: 313–324.

165 The differences between national European legislation based on the European Union's Data Privacy Directive in contrast to an industry self-regulation approach found in the United States are well-known. Since this distinction is not part of this study it is not explained in further detail in the report.

166 Iyengar, S.S.; Lepper, M.R. (2000): When Choice is Demotivating: Can One Desire Too Much of a Good Thing?. Journal of Personality and Social Psychology. Vol. 79, No. 6: 995 -1006. The same point is made in a publication by the UK Better Regulation Executive and National Consumer Council in 2007: Warning: Too much information can harm. A final report by the Better Regulation Executive and National Consumer Council on maximising the positive impact of regulated information for consumers and markets. For an approach to better information practices also Ofcom (2013): A Review of Consumer Information Remedies. Research Document, 12th March 2013. London.

settings even though they are not able to grasp their meaning (from an economic point of view, they assume very high opportunity costs).

Sadeh et al.[167] also suggest an approach for combining linguistic analysis and crowdsourcing technologies in order to develop a tool for semi-automatically extracting key features from existing natural language website privacy policies. They intend to use innovative user interfaces for the presentation of those policies. Ammar et al. follow a similar approach with their research on how consumers can extract noteworthy terms of privacy policies automatically.[168] The researchers used annotated privacy policies from the crowdsourced Terms Of Service Didn't Read project (tosdr.org), and they collected 794 additional privacy policies without annotations. By using logistic regression, they mapped the privacy policy documents to the extracted categorical labels (e.g. "Deleted images are not really deleted", "Using your real name is optional"). As a result, they demonstrated that their pilot software is capable of answering selected questions about privacy policies. However, the authors recognise that further work would be needed to turn this into a tool that can be used more widely.

Driven by the insight that consumers do not learn about the content of terms via reading them (all), Ayres and Schwartz[169] tested the premise that consumers learn about them in a recursive process. Their hypothesis is that consumers gain knowledge about terms and conditions through past experience, learning from each other, from experts and so forth. Ayres and Schwartz validated this hypothesis in a study on consumer expectations about Facebook. The researchers postulated that users often "expect more favourable terms than they actually receive".[170] As a result, they proposed a system under which service providers (e.g. social network providers like Facebook) are required periodically to check if consumers actually understand the terms of their agreement.

Consequently, the authors suggest that businesses should aid consumers in their cognitive process with vivid disclosure in a form of standardised warning boxes (a process which they call substantiation) that nudge the users to particularly important terms that they are likely to care about. Five or even fewer items appear sufficient for such warning boxes. This technique of disclosure has the benefit of not overwhelming consumers with information while at the same time giving them a realistic picture of unexpected terms.

---

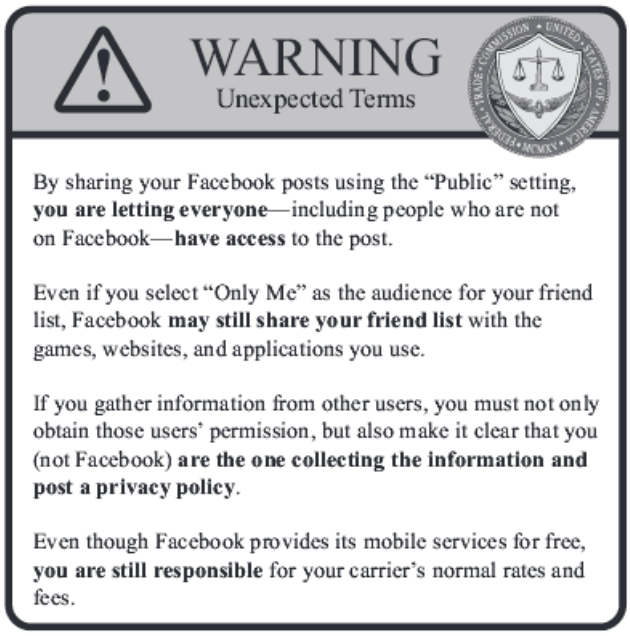
167 Sadeh, N.; Acquisti, A.; Breaux, T.D.; Cranor, L.F.; McDonald, A.M.; Reidenberg, J.R.; Smith, N.A.; Liu, F., Russell, N.C.; Schaub, F.; Wilson, S. (2013): The Usable Privacy Policy Project: Combining Crowdsourcing, Machine Learning and Natural Language Processing to Semi-Automatically Answer Those Privacy Questions Users Care About. December 2013, Research paper CMU-ISR-13-119.

168 Ammar, W.; Wilsony, S.; Sadehy, N.; Smith, N.A. (2012): Automatic Categorization of Privacy Policies: A Pilot Study. School of Computer Science, Carnegie Mellon University PA 15213.

169 Ayres, I. and Schwartz, A. (2014): The No Reading Problem in Consumer Contract Law, Stanford Law Review 2014: 545-600.

170 Ibid. 545, 571ff. The authors see causes for term optimism in consumer inexperience, cognitive bias, or seller advertising.

Figure 4-3: Example of warning box according to Ayres and Schwartz



Source: Ayres and Schwartz (2014), p. 601.

Mitts' study[171] further underpins the positive effect of similar disclosure boxes. They improved consumer understanding of terms and conditions by 9 to 10%. More than five items in such warning boxes did not improve understanding. Furthermore, it was found that increasing the number of warnings is likely to annoy consumers and drive them away from the website.

Although at least some of the approaches to condense information on terms and conditions into a label, icon or similar format show some promising results, there are some fundamental issues that have to be considered if one intends to follow such an approach. First and foremost, the reader should keep in mind the transparency paradox coined by Nissenbaum (see section 3.2) that highlights the contradiction between the legal necessity to inform the consumer in detail and the objective of presenting the information in a format that actually enables consumers to read and understand terms and conditions.

In a similar vein, it can also be argued that there is contradiction between companies natural interest to build "liability shields" and consumers' interest to be informed about the most important cornerstones of a specific privacy policy. Consequently, companies often use "long texts that are too legalistic and complicated"[172] for privacy policies.

171 Mitts, J. (2014): How Effective is Mandatory Disclosure? Columbia University. Working paper.

172 Coopamootoo, P.L.; Ashenden, D. (2011): Designing usable online privacy mechanisms: what can we learn from real world behaviour?. Privacy and Identity Management for Life. IFIP Advances in Information and Communication Technology (Volume 352): 311-324, 316.

Interestingly, from a legal perspective, information that is too detailed, technical and lengthy might not violate data protection regulations as such but could lead to high risks to the privacy of users as they consent to something that hides its meaning more or less deliberately from them. Representatives from the data protection authorities of each EU member state, the Article 29 Working Party, strongly disapprove of long privacy policies full of legalese. In a letter to Google Inc. they criticise the company's new privacy policy and explicitly state that in general "Internet companies should not develop privacy notices that are too complex, law-oriented or excessively long".[173]

Further standardisation of data protection regulations and provisions for privacy policies may help reduce consumers' costs for reading and understanding. More harmonised information provisions in the EU or even internationally could help to reach this aim. In 2012, the European Commission's proposal for a new data protection regulation mentioned such a requirement.[174] Such a provision might reduce complicated legal language in privacy policies, and it might make it easier to impose regulations on a national level.

Some countries have already adopted laws governing how information on public administration websites needs to be presented. For instance, in 2011 Germany implemented a provision for barrier-free access to digital information. Since then, national government institutions have been obliged to offer digital information not only for disabled people but also in "easy-to-understand language". Website users can easily switch from elaborate to simpler code.[175] Other institutions and companies have followed the example.[176] However, it remains to be seen whether this approach will be widely adopted.

In the USA, government institutions have been investigating ways in which smart disclosure may empower consumers and increase market transparency.[177] Expanding the use of smart disclosure is a declared objective of the Federal Government. In particular, the Federal Government aims to improve and promote access to smart disclosure data; to encourage companies to make more information about their

173 The French data protection authority CNIL had conducted an investigation on revised Google privacy policies, see Article 29 Working Party (2012), Letter to Google. 16.10.2012: 2. Zuiderveen Borgesius, F. J. (2015): Improving Privacy Protection in the Area of Behavioural Targeting (PhD thesis University of Amsterdam), Kluwer law International (forthcoming).

174 Art 11 of the European Commission proposal for a Data Protection Regulation (2012), see section 3.1. Cf Zuiderveen Borgesius, F. J. (2015): Improving Privacy Protection in the Area of Behavioural Targeting (PhD thesis University of Amsterdam), Kluwer law International (forthcoming).

175 The main objective was to offer access to information for disabled persons (i.e. blind people), people with learning difficulties or non-native readers. The law is a means to foster an inclusive society. Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie-Informationstechnik-Verordnung - BITV 2.0). So far there has been no overall scientific examination of the effectiveness of this regulation in practice.

176 See e.g. http://www.nachrichtenleicht.de/ (news provider); http://www.dhm.de/leichte-sprache/ (museum), http://www.bundestagswahl-bw.de/leicht.html (information on general election); www.bundesbank.de (federal bank);

177 The Task Force on Smart Disclosure: Information and Efficiency in Consumer Markets (2013): Smart Disclosure and Consumer Decision Making: Report of the Task Force on Smart Disclosure.

products and services directly available to consumers; and to make the personal data they collect securely available to individuals. In the end, this should enable the consumer to make his/her own consumer-facing choice engines.[178]

In this context, the Better Information Handbook[179] presents a practical approach to improving the understanding of legal information. This publication, funded by the Ministry of Justice in the UK, compiles the issues involved in the successful delivery of information to the public. Information should be accurate, up to date and in plain English. Moreover, information has to be built around the needs of the audience, which implies that dissemination and message have to be matched and that the effectiveness of the information has to be evaluated.

Although all of the above appear to be crucial requirements, it remains unclear how they may be incorporated in privacy policies since they might not line up with the interests of website providers. How a *regular* and sustainable evaluation of a third party's perception of privacy policies could contribute to more consumer awareness is a key question that needs addressing. This approach takes into account the need for communication between data protection experts and consumers in order to come to a mutual understanding of what a consumer perceives and how a website provider is actually processing data.[180] It also acknowledges the fact that privacy in the digital society is an evolving topic: new devices, new services and new user clusters require a review of the understanding and the means to achieving an acceptable data protection level for consumers.

Finally, regular updating and evaluating of existing knowledge about privacy is required in order to keep pace with changing policies and technological trends. As a consequence, we would argue that consumer information in the field of personal data and privacy may not assume static technological and regulatory context; rather, it should consider regular revisions.[181]

178 Thaler, R. H.; Tucker, W. (2013): Smarter Information, Smarter Consumers. Harvard Business Review, January-February: 44-54.

179 Webber, M.; Harris, T.; Jones, M. (2009): Better Information Handbook. Advice Services Alliance. London. The authors give examples of good practices, see e.g. 28ff.

180 The CMA in the UK is currently running a call for information to get to know more about companies' data collecting and processing, see CMA – Competition & Markets Authority UK (2015): Call for information - The commercial use of consumer data. London.

181 Other practical guidebooks have followed a similar approach, e.g. Richie, Al; Corrigan, J.; Graham, S.; Hague, A.; Higham, A.; Holt, J.; Mowbray, P. (2011): Transforming consumer information A study conducted by the Consumer Information Working Party, 26 October 2011, Working paper.

How to improve understanding?

- *The experimental studies on how to make terms and conditions easier to comprehend show a range of results as regards whether labels icons and similar measures can really resolve the issues of reading and understanding terms and conditions.*
- *Privacy policies that reflect a consumer's individual cultural background and preferences contribute to better understanding. Software solutions are being developed to automatically extract and contextualise privacy policies to meet this requirement.*
- *Warnings about unexpected terms in a privacy policy may serve as a means to help consumers become aware of unusual practices.*
- *More harmonised information provisions could help reduce consumers' costs for reading and understanding. Various government initiatives exist to set guidelines for improving privacy policies.*

4.3 How to improve the chance that consumers act upon information?

The previous sections have discussed that approaches to improve readership and understanding of terms and conditions show heterogeneous results. However, there appears some concurrence across studies that a more contextualised and adaptive approach may be required. Such an approach would have to account for the possibility that both privacy policies and consumers' preferences may change over time. In line with this thought, "nudging" can be considered one of the predominant ideas discussed among behavioural economists, psychologists and data protection representatives to help remind people of their choices and options continuously. One may expect that regular reminders may trigger more context-aware decisions and hence actions. Naturally, the format of such nudges has to draw from the findings of studies discussed in previous sections in order to be as effective as possible without compromising the quality of information.

Although some researchers may consider nudging a means to confront consumers' irrationality effectively, it is unlikely that this measure will actually resolve consumers' irrationality. This is because nudging consumers towards privacy can show them ways that are in accordance with their own privacy interests. This happens through confronting consumers with the need to responsibly expose their personal data and at the same time offering alternatives. Thus, a "nudge" would preserve the possibility to choose to share personal data as well as allowing the consumer not to reveal too much data at the same time. Thaler and Sunstein use the term "libertarian paternalism" in this

context to show how freedom of choice and effective regulation may go hand in hand.[182] While legislative frameworks imply an a priori limitation of service providers' options to collect and process data, nudging enables any kind of business model based on personal data as it does not compromise consumers' freedom of choice.

For more than ten years, researchers like Acquisti have applied theories and methodologies from behavioural economics and behavioural decision research to investigate decision-making. In this context, the main objective is to identify inconsistencies in privacy choices, constitute conclusive explanations and try to "build better privacy technologies and information policies".[183] Nudging privacy has proven to be one of the promising approaches in many experiments.[184] The following paragraphs give some detail on such experiments.

Wang et al. examine whether it is possible to help users of a SNS (Facebook) to avoid posting embarrassing messages, i.e. over-sharing personal information they later regret.[185] In an experiment they designed three potential privacy nudges[186]: (1) the "profile picture nudge" where they display five profile pictures and a message stating "These people, your friends, AND FRIENDS OF YOUR FRIENDS can see your post"; (2) the "timer nudge", a short time delay before a post is actually posted; and (3) the "sentiment nudge", where after the consumer clicks the post button, a timer and a note with a yellow background is shown. Although the field trial was exploratory and more trials might be required, the authors conclude that as a result of the experiment, privacy nudges can be a powerful instrument to make consumers think about the consequences of their postings.

Balebako et al. have explored "nudging users towards privacy on mobile devices", to help consumers with decisions regarding the sharing of location data.[187] There is also a recent study on nudging consumers to avoid installing privacy-invasive smartphone

182 Richard H. Thaler, R.H.; Sunstein, C.R. (2003): Libertarian Paternalism, 93 Am Econ Rev 175 (May 2003): 175-179.

183 Acquisti, A. (2009): Nudging Privacy. The Behavioral Economics of Personal Information. Security & Privacy Economics IEEE (November/December 2009): 72-75 (pre-publication version). For an overview see also Acquisti, A. (2010): The Economics of Personal Data and the Economics of Privacy. Background Paper No. 3, Joint WPISP-WPIE Roundtable: "The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines", 1 December 2010.

184 The approach is also elaborated in detail in Zuiderveen Borgesius, F. (2015): Behavioural Sciences and the Regulation of Privacy on the Internet Nudging and the Law - What can EU Law learn from Behavioural Sciences?. Sibony A.-L., Alemanno, A., eds. (forthcoming). A working paper on this topic has been presented at the 6th Annual Privacy Law Scholars Conference (Berkeley, 7 June 2013), and the Nudging in Europe Conference (Liège, 12-13 December 2013).

185 Wang, Y.; Leon, P.G.; Chen, X.; Komanduri, S.; Norcie, G.; Scott, K.; Acquisti, A.; Cranor, L.F.; Sadeh, N. (2013): The Second Wave of Global Privacy Protection: From Facebook Regrets to Facebook Privacy Nudges. 74 Ohio State Law Journal 1307, p 1307-1335 and Wang, Y.; Leon, P. G.; Acquisti, A.; Cranor, L. F.; Forget, A.; Norman Sadeh, N. (2014): A Field Trial of Privacy Nudges for Facebook. CHI 2014 , Apr 26 – May 01 2014, Toronto, ON, Canada, ACM 978-1-4503-2473-1/14/04.

186 For a detailed description see Wang, Y. et al. (2013): 320 ff.

187 Balebako, R.; Leon, P.G.; Almuhimedi, H.; Kelley, P.G.; Mugan, J.; Acquisti, A.; Cranor, L.F.; Sadeh, N. (2011): Nudging users towards privacy on mobile devices. Proc. CHI 2011 Workshop on Persuasion, Nudge, Influence and Coercion.

apps.[188] Study results by Choe et al. suggest that when a mobile application's privacy is shown as a visual rating, consumers are able to understand the "nudge" and act accordingly. They recommend using familiar positive visuals (e.g. the colour green, plus signs or thumbs up).

Most recently Almuhimedi et al. conducted a field study to find out if a fine-grained mobile app permission manager could be an effective way of helping users review and modify their permissions and if privacy nudges – regular alerts in the form of messages – could enhance the effectiveness of this tool.[189] At first, in the experiment solely AppOps for Android was used, then, the researchers added privacy nudges integrated as click-boxes. From the authors' point of view[190] the results confirm that consumers are not really aware of collection practices of mobile app providers but that a fine-grained permission manager proved to be beneficial and its effectiveness could be even enhanced by nudges in click-boxes saying "Let me change my settings" or "Show me more before I make changes".

Another "nudging" approach might be to leverage opt-in options according to the level of how consumers rate details of their personal data, i.e. name, address, mobile phone number, location data, photographs, etc. Perhaps one mouse click to opt in could be enough to consent to use basic personal data or maybe data perceived as non-invasive. More mouse clicks could be required to confer the right to use more personal data. "Sticky defaults", according to Ayres, could be an "intermediate category falling between ordinary defaults and traditional mandatory rules".[191]

Whether such measures would effectively improve the protection of consumer privacy depends on consumers' choices, which might still be influenced by biases. Acquisti et al. point out how eventually even simpler or more usable privacy controls and notices may not improve consumers' decision-making.[192] Nudging will not prevent consumers from making paradoxical choices as their perception of risks can vary depending on the context. As a result of a corresponding experiment, Brandimarte et al. summarise the consequences of this paradox as follows: "Our findings have both behavioral and policy implications, as they highlight how technologies that make individuals feel more in

188 Choe, E. K.; Jung, J.; Lee, B.; Fisher, K. (2013): Nudging people away from privacy-invasive mobile apps through visual framing. Human-Computer Interaction–INTERACT. Springer.

189 Almuhimedi, H.; Schaub, F.; Sadeh, N.; Adjerid, I.; Acquisti, A.; Gluck, J.; Cranor, L.; Agarwal, Y. (2015): Your Location has been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging. CHI 2015, April 18 - 23 2015, Seoul, Republic of Korea: 1-10.

190 I.e. the authors of the present study.

191 Ayres I. (2012): Regulating Opt Out: An Economic Theory of Altering Rules. 121 Yale L.J. 2032 (2012): 2087. Cf. Zuiderveen Borgesius, F. J. (2015): Improving Privacy Protection in the Area of Behavioural Targeting (PhD thesis University of Amsterdam), Kluwer law International (forthcoming).

192 Acquisti, A.; Adjerid, I.; Brandimarte, L. (2013): Gone in 15 Seconds: The Limits of Privacy Transparency and Control. Security & Privacy, IEEE (11/ 4): 72-74.

control over the publication of personal information may have the paradoxical and unintended consequence of eliciting their disclosure of more sensitive information."[193]

Apart from "nudging", charged privacy services and differentiated opt-in options, other options include allowing consumers to specify privacy preferences while using the service (or, if they are registered users, establish their own profile).[194] In this context, Cranor emphasises how a more sophisticated approach might allow consumers to create "multiple personae".[195] It seems obvious that this possibility could fulfil demands for a personalised but at the same time more privacy-friendly service from the consumer's and from the provider's point of view. Another option that is sometimes discussed is to offer different versions of a service and to charge a fee for the less privacy-invasive version.[196] On the one hand, this will draw consumers' attention to data-processing issues in general. On the other hand, this would enable consumers to compare the prices they have to pay for more privacy across similar websites or services they would like to use.

Finally, it should be noted that while new developments in digital media may also have a positive impact on consumer privacy as they can enhance their position in negotiating privacy concerning general as well as specific issues.[197] Via video, blog entry, tweet or Facebook post, individual consumers are able to publish their opinions on privacy and to protest against, for example, changes in terms of contracts. Consumers can generate more attention on a certain topic, network with other consumers and eventually a provider might be more easily forced to react than in the offline world. Digital publication of information and arguments can result in enormous pressure on the "data collectors". We would see information and the potential response of the public as one necessary but not sufficient tool of consumer empowerment.

---

193 Brandimarte, L.; Acquisti, A.; Loewenstein, G. (2010): Misplaced Confidences: Privacy and the Control Paradox. Ninth Annual Workshop on the Economics of Information Security (WEIS). June 7-8 2010: 1

194 This option is described by LF Cranor as a means to come to accepted personalised profiles while doing online shopping, see Cranor, L.F. (2003): 'I didn't Buy it for Myself': Privacy and Ecommerce Personalization. Proceedings of the ACM Workshop on Privacy in the Electronic Society, Washington, DC, October 30.

195 Ibid.

196 See the comprehensive discussions in the European CEPS DIGITAL FORUM that also include a possible impact of cost-benefit analysis, Irion, K.; Luchetta, G. (2013): Online Personal Data Processing and EU Data Protection Reform. CEPS Task Force Report of the CEPS Digital Forum 2013: 38.

197 This argument is discussed in detail in an article by Barnes, W. R. (2012): Social Media and the Rise in Consumer Bargaining Power. University of Pennsylvania, Journal of Business Law (Vol. 14:3 2012): 661-699. See also Dreyer, S.; Ziebrath, L. (2014): Participatory Transparency in Social Media Governance: Combining two Good Practices. Journal of Information Policy, Vol. 4, 2014: 529-546.

How to improve the chance that consumers act upon information?

- *Nudging consumers towards privacy is a "choice-preserving" approach. Consumers are free to make their own decisions but they are shown potential consequences of different privacy options.*
- *"Nudges" should be chosen according to the devices or services used.*
- *Allowing consumers to specify privacy preferences while using the service can improve privacy and allow a more personalised service according to the requirements of the consumer.*
- *A new – but not sufficient – tool for consumer empowerment could be to publish opinions on privacy and to protest against, for example, changes in terms of contracts in social networks or other digital services. Thus, digital media can enhance consumer bargaining powers.*

4.4 Informed consent could be improved by learning from a domain that made it work

The analysis in the present chapter has focused thus far on informed consent in relation to digital and data-driven products and services. There may in addition be relevant insight to be obtained from informed consent in other domains. Clinical research appears to be a specially suited case to look at and to discern whether this domain found ways to actually make informed consent work.

There are strong reasons for why clinical research qualifies as an area to provide relevant context to the domain this study focuses on. Clinical research has come a long way. It is a field with a long and rich tradition – certainly much longer than the period in which online services or mobile apps have become widespread. It does not come as a big surprise that the debate on informed consent has been led by clinical research. For example, even the term "informed consent" is dominated by clinical or otherwise health-related research on human subjects.

Dealing with informed consent for longer than others does not necessarily imply that one may have found a solution to make it work. Being able to occupy the term may serve as a stronger indicator that the domain has made progress, but it is also not sufficient on its own. However, two factors provide evidence that the clinical field's long-running debate on informed consent did indeed bear fruit. First, clinical research reached consensus along crucial dimensions defining informed consent and a working model of the informed consent process. Second, there is internationally harmonised regulation that reflects this consensus. The regulation comes in the form of good

practices such as Good Clinical Practice (GCP).[198] Demonstrating compliance with GCP (and any related national applicable law) is a mandatory requirement to conduct clinical research and for drug approval.

It is important to note that we do not intend to imply that there should be a comparable internationally harmonised regulation governing how informed consent is to be understood and implemented for digital and data-driven products and services. The key insight in comparing both domains is that clinical research is indeed further down the road. Most notably, there is substantial indication that clinical research has found solutions to the issues that people do not read lengthy and difficult-to-understand terms and conditions, that they do not understand them when left on their own, and that they by and large do not act upon reading.

These issues are equally relevant to both domains. Regarding people's lack of understanding, the Belmont Report[199] analyses that the informed consent process in clinical research builds not only on the principles of information and voluntariness, but also on comprehension. The Declaration of Helsinki,[200] the foundation of GCP, addresses this issue as it mandates that the subjects of a clinical trial must be "informed participants". Similarly, the International Ethical Guidelines for Biomedical Research Involving Human Subjects[201] defines informed consent as "[…] a decision to participate in research, taken by a competent individual who has received the necessary information; who has adequately understood the information; and who, after considering the information, has arrived at a decision without having been subjected to coercion, undue influence or inducement, or intimidation."

As a result clinical research has chosen a much more active informed consent process. When people do not read, understand and act, the informed consent process in clinical research has been designed to *make* them understand. In addition to the requirements to provide information that is easy to understand and to take cultural and societal context into account (e.g. people who are not able to read), the informed consent process in clinical research always includes a specific consent interview. This means that in each and every case a meaningful exchange takes place, which allows potential participants to ask questions, to take ample time to consider their decision, and to receive answers from a competent person. This differs substantially from the informed consent process in our domain.

---

198 International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use (1996): Guideline for Good Clinical Practice. ICH Harmonised Tripartite Guideline, E6(R1): 1-59.

199 The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research (1978): The Belmont Report. Ethical Principles and Guidelines for the Protection of Human Subjects of Research: 1-40.

200 World Medical Association (2013): WMA Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects. 7th revision.

201 Council for International Organizations of Medical Sciences (2002): International Ethical Guidelines for Biomedical Research Involving Human Subjects.

The World Health Organization (WHO) provides relevant guidelines that address the question of how investigators of a clinical trial ensure that participants in a consent interview have understood the information they receive. In their guidelines, the WHO cross-refers to the International Ethical Guidelines for Biomedical Research Involving Human Subjects:

"Informing the individual subject must not be simply a ritual recitation of the contents of a written document. Rather, the investigator must convey the information, whether orally or in writing, in language that suits the individual's level of understanding. The investigator must bear in mind that the prospective subject's ability to understand the information necessary to give informed consent depends on that individual's maturity, intelligence, education and belief system […] The investigator must then ensure that the prospective subject has adequately understood the information. The investigator should give each one full opportunity to ask questions and should answer them honestly, promptly and completely. In some instances the investigator may administer an oral or a written test or otherwise determine whether the information has been adequately understood."[202]

We would argue that the field of informed consent in privacy has yet to address the question of whether there is the need to actively ensure consumers' comprehension. If there were to be consensus on this issue, the above guidelines from clinical research could perhaps determine a model to consider towards achieving informed consent in privacy. However, the clinical research model differs from current practice in respect of data privacy in three important respects:

- It would impose the burden on providers to ensure that consumers understand and come to an informed decision;
- It would endorse individualised communication; and
- It would endorse interaction.

The key challenge in adopting such a model in the context of privacy issues would obviously be the resulting transaction costs[203] (costs incurred by making an economic exchange) for providers as they would have to undertake additional steps in order to fulfil their duty to make sure consumers comprehend. Transaction costs would be substantial if all of the above three dimensions were applied on a mass scale in the business-to-consumer markets for digital/data-driven products and services. In

202 WHO (2002): International Ethical Guidelines for Biomedical Research Involving Human Subjects. Prepared by the Council for International Organizations of Medical Sciences (CIOMS) in collaboration with the WHO. Geneva: 33.

203 Transaction costs are "any costs connected with the creation of transactions themselves, apart from the price of the good that is the object of the transaction" (Luth, H. A. (2010): Behavioural Economics in Consumer Policy: The Economic Analysis of Standard Terms in Consumer Contracts Revisited (PhD thesis University of Rotterdam) (Academic version 2010), p 19). See also: Coase, R.H. (1960): The Problem of Social Cost. Journal of Law and Economics. Vol. 3 (Oct., 1960): 1.

particular, the second and third dimensions would need providers to move away from general terms and conditions and to move away from (effectively) unidirectional information. The first dimension may, on the other hand, be adopted without the second and third ones in order to mitigate so as to keep the expected increase in transaction costs under control: introducing a number of test questions may allow a provider to make sure consumers understand the minimum information needed to make an informed decision.

Whether or not the domain of data privacy and data sharing would be ready to adopt the above model (fully or in parts) will essentially depend on whether it is able to reach a consensus on the trade-off between risks and benefits for consumers to use digital and data-driven products and services. At this point in time, there does not appear to be enough information to assess risks and benefits. What is known, however, is that consumers are unaware about what happens to the data they provide when using an online service and that their expectations deviate from actual practice.

We noted at the beginning of this section that clinical research has led the debate on informed consent for quite some time. Further, with respect to naming and assessing risks and benefits for trial subjects, clinical research is substantially more developed than the area of data privacy and data sharing. Reaching this position has been a long, tedious and at times painful process. As a matter of fact, the requirement for informed consent was not been recognised in clinical research for a long time. It took a long list of historical cases[204] to come to the attention of researchers, courts and society at large before the area could establish a notion of right and wrong, of what is ethical and that human trial subjects had rights after all. The latter insight was key for clinical research to realise and accept that trial subjects must be informed about the relevant risks, the benefits and any alternatives prior to a trial beginning.

As much as it was a challenge for clinical research, it will be challenging for the area of data privacy and data sharing to establish a widely accepted understanding of relevant risks and benefits to consumers. However, if informed consent is to be taken seriously, there is no way around this debate. If the goal is that consumers should be able to make informed decisions, the lesson from clinical research is that firms need to ensure that consumers understand and that to make clear the relevant risks and benefits for consumers when they choose to use a digital and data-driven product or service.

In conclusion, there are two key lessons to be learned from assessing the informed consent process in clinical research. Both relate directly to the respective factors that appear as the main contributors to make informed consent work. The first factor refers to information asymmetry and how to overcome it, namely by imposing a duty to ensure consumers' understanding. The specific modalities need to be considered carefully due

204 For an exemplary presentation of the history of informed consent in clinical research see: Presidential Commission for the Study of Bioethical Issues (2014): Informed Consent Background: 1-17.

to an imminent risk of increased, potentially excessive, transaction costs. For instance, it would appear unrealistic to assume that the interactive process established in clinical research to obtain informed consent could be transposed into the area of data privacy and data sharing without any adaptations: individual face-to-face communication would not scale with the requirements of a mass market. However, if other approaches to improving informed consent (as discussed in previous sections of this report) do not achieve the desired outcome, it seems difficult to avoid accepting some increase of transaction costs in order to secure consumers' understanding. Lightweight means, such as introducing a number of test questions, might help keep transaction costs within reasonable limits.

However, the key to agreement on an acceptable level of costs is likely to depend on the second factor, namely whether we can agree on the risks and benefits that consumers derive from using online services. Clinical research went through a decades-long painful process before finally reaching agreement on the importance of trial participants understanding both the risks and the benefits. As a result, clinical research has accepted significant transaction costs in order to ensure informed consent. This would suggest that a key first step in thinking about how such an approach could be adapted to online services, there would need to be agreement on the risks and benefits to consumers. Such agreement would need to reflect a consensus on socially and economically acceptable behaviour in the data-driven economy, especially with respect to data harvesting, forwarding, aggregation and analytics practices. As we know that consumers are unaware even about relatively simple analytics techniques (for instance that their browsing history is analysed; see section 3.1), it will be interesting to learn about how consumers value more advanced techniques – and how they would express the potential of these techniques in terms of a risk/benefit trade-off. We are by no means implying that this trade-off is negative; what we want to emphasise is that risks and benefits appear mostly unexplored today – which appears to be the obvious result of unaware consumers and the widespread use of data harvesting and processing practices that take place in secrecy. Delineating right from wrong thus will be an essential part of naming risks and benefits to consumers. Valuing risks and benefits will, in turn, be an essential part of defining how serious we actually take informed consent as a requirement. This valuation – in combination with the assessment whether other means to improve informed consent have the desired effect – will be an important consideration in determining whether providers need to take measures to ensure that consumers understand the risks and benefits, and under what circumstances providers might need to document that consumers understood.

How to improve informed consent by learning from a domain that made it work?

- *In realising informed consent's importance, it will be essential to establish an agreed notion of relevant risks and benefits to consumers when using online services.*
- *Given that people by and large do not read and understand privacy policies - , and should other ways to improve informed consent fail to have the desired effect ,- the informed consent process may need to be designed in a way to ensure that consumers read and understand.*
- *A model for such an informed consent process may deviate from the current process by imposing a burden on providers to ensure that consumers understand and come to an informed decision. The specific circumstances need to be carefully considered in order to keep transaction costs within reasonable limits (for instance by lightweight means such as introducing a number of test questions).*

5 Conclusions and possible future research

This study sought to understand (1) the role of informed consent in privacy law, (2) the role of informed consent in practice and (3) potential ways to improve informed consent in practice. Furthermore, the study investigated the impact of the Internet of Things on the three major issues.

With regard to the first two research questions, it was found that there is a fundamental dissonance between the assumptions and requirements for informed consent as stipulated in law and actual consumer behaviour in practice. Whereas privacy law rests on the assumption that consumers give informed consent, which means that they have read and understood the agreement they enter, in practice consumers commonly do not read terms and conditions, and they are also not able to understand the concepts, contents and consequences. These points are not disputed in the literature. In fact, "[t]he literature on the inadequacy of privacy policies is well-documented, and, we think, conclusive enough that it does not need to be continued".[205]

Besides confirming the inadequacy of privacy policies, this literature review finds that even if consumers read and understood privacy policies, they would still have very little scope to evade online tracking technology that is becoming more and more sophisticated. However, it has also been shown that consumers have developed strategies of advertising avoidance and resistance to cope with the currently most prominent effect of online tracking: targeted online advertising.

Whether consumers actually make the link between data gathering and analysis and the targeted advertisements that they receive, for instance, on their SNS profiles is, however, questionable. For instance, a study by Cranor and McDonald[206] found that significantly less than half of web users (40%) were aware that their email messages may be scanned to enable targeted advertisements. Furthermore, 29% of users in the same study did not believe that this was actually common practice as they thought such practices would be unlawful.[207] This lack of awareness may explain that although consumers consistently show a high level of concern about their personal data and the protection of it, they do not read terms and conditions or more specifically privacy policies. This is commonly referred to as the "privacy paradox".

In light of these deficiencies, various studies have aimed to develop approaches that can tackle the individual steps of reading, understanding and acting in the context of

205 Doty, N. and Gupta. M. (2013): Privacy Design Patterns and Anti-Patterns. Symposium On Usable Privacy and Security (SOUPS) 2013, A Turn for the Worse: Trustbusters for User Interfaces Workshop: 2.

206 McDonald, A.M.; Cranor, L.F. (2010): Beliefs and Behaviors: Internet Users. Understanding of Behavioral Advertising (38th Research Conference on Communication, Information and Internet Policy (Telecommunications Policy Research Conference)) (2 October 2010).

207 Cf Zuiderveen Borgesius, F. J. (2015): Improving Privacy Protection in the Area of Behavioural Targeting (PhD thesis University of Amsterdam), Kluwer law International (forthcoming).

informed consent for personal data processing. Commonly, these approaches set out to develop a more palatable format of privacy policies. They condense information, use software tools to summarise privacy policies automatically or develop privacy seals and labels that mimic fair trade or organic labels known in the food industry. However, such labels have been shown to trigger misconceptions in consumers about the protection of their personal data. Furthermore, Nissenbaum rightly points out that this approach may be misleading as "transparency of textual meaning and transparency of practice conflict in all but rare instances".[208]

More sophisticated approaches account for the changing context for both consumers' privacy preferences and privacy policies. In line with the idea of privacy labels, Bashir et al.[209] integrate these ideas into their Knowledge-based Individualized Privacy Plan (KIPP). KIPP aims to improve consumer comprehension of the significance of privacy notices by personalising information based on different levels of pre-existing knowledge.

Another context-aware approach that addresses both consumer understanding and action in the context of informed consent is so-called "nudging". It is one of the predominant ideas discussed among behavioural economists, psychologists and data protection representatives to help remind people of their choices and options continuously. Thus, it can trigger consumer action that is appropriate to the current context and preferences. As such, this may prevent consumers from making choices they might regret later. However, it has also been shown that too many such nudges may mitigate their effect. Nudging consumers towards privacy is a "choice-preserving" approach. Consumers are free to make their own decisions but they are shown potential consequences of different privacy options. Thus, it strikes a balance between consumers' interests and enabling new (and evolving) business models based on personal data processing.

Contextualising seems promising as some studies in this literature review have shown that privacy concerns (privacy involvement), self-efficacy and other personal characteristics shape one's concept of privacy just as much as one's cultural background is likely to do. Furthermore, it has to be understood that privacy is an evolving concept. This can be illustrated by early papers which date back to the time when photography became more popular and was seen then as a significant threat to privacy and possibly society itself. We can expect the concept of privacy to undergo further changes as our technological environment develops. Although the present literature review has not explored the literature on the conceptualisation of privacy through time, it is still noteworthy that only a few studies from the realm of behavioural

208 Nissenbaum, H. (2011): A Contextual Approach in Privacy Online. Daedalus 140(4): 36.
209 Bashir, M.; Hoff, K.A.; Hayes, C.M.; Kesan, J.P. (2014): Knowledge-based Individualized Privacy Plans (KIPPs): A Potential Tool to Improve the Effectiveness of Privacy Notices", Workshop on the Future of Privacy Notice and Choice, Carnegie Mellon University June 27, 2014.

economics seem to address this point or account for it. Here, we would suggest that this is an area where more work could be done.

The concept of privacy will also help determine which elements of personal data tracking consumers perceive as being invasive. In this report, we have found several studies providing evidence for consumer advertising avoidance or resistance strategies. Such behaviour appears to be particularly prevalent when consumers perceived the advertisements as cluttered, intrusive and irritating. With more and more business models hinging on the funding gained from targeted advertising, such avoidance and resistance strategies (if successful) cast doubt on targeted advertising as well as the tracking of personal data necessary to conduct it. Future research could investigate if the real market for privacy can possibly be negotiated at the level personal data tracking effects (e.g. targeted advertising) rather than at the level of data harvesting.

While targeted advertising is currently the most common use of personal data, it is hardly the only option imaginable. Besides positive effects such as identification of cures for diseases from big data analysis, there may also be adverse effects such as identity theft. As these effects are not yet fully understood, it may also be difficult to solve the problem of consumer uncertainty about the consequences of agreeing to a privacy policy. Consequently, investigating current and future ways to exploit personal data commercially and otherwise constitute a possible area for future research.

Such insights may also tackle the more fundamental issue of consumers' awareness, which we feel lies at the heart of the controversy around privacy and personal data. This goes hand in hand with Helberger's[210] remark that consumer information is not a one-time act but a process, and future research could address the phase of the consumer information process before they even come in contact with terms and conditions, namely when they become aware that there is an issue at all. Awareness is likely to motivate consumers to engage with terms and conditions and in particular privacy policies of services and products they consume. As the Elaboration Likelihood Model[211] predicts, higher motivation leads to more systematic and detailed information processing focusing on a high-quality argument instead of heuristic cues. Thus, with increased awareness, consumers may be significantly more likely to actually engage with terms and conditions. Given this, the present study has presented some promising ways to facilitate reading and understanding as well as helping consumers make the right decisions at the right time.

Another potentially promising avenue for future research may be to learn from other disciplines that already have solutions to make informed consent work. We have

210 Helberger, N. (2013): Form Matters: Informing Consumers Effectively. Amsterdam Law School Research Paper No. 2013-71/Institute for Information Law Research Paper No. 2013-10.

211 Cacioppo, J. T.; Petty, R. E. (1983). Social psychophysiology: A sourcebook. New York: Guildford Press.

referred to the example of clinical research where it was first necessary to establish the actual risks if informed consent was not actual informed consent. It took a long list of – from today's perspective – unethical and quite frightening cases to come to the attention of researchers in the domain, courts and society at large before the domain could establish a notion of right and wrong, of what is ethical and that human trial subjects have rights after all. As much as it was a challenge for clinical research, it will be challenging for our domain to establish a widely acceptable understanding of relevant risks and benefits to consumers. However, if informed consent is to be the benchmark, there is no way around this debate in our domain. If the goal truly is that consumers make informed decisions, we can learn from clinical research that we have to make consumers understand and that we have to be able to specify relevant risks and benefits for consumers when they choose to use a digital and data-driven product or service.

In the annex to this study, we discuss the relevance of personal data and informed consent in the light of the evolution towards the Internet of Things.

6 Annex: Internet of Things and personal data

The Internet of Things (IoT) is about ubiquitous digitisation. It builds on data flows from and to devices that were previously unconnected. In the same way the Internet forms a network of previously unconnected networks, the IoT enables the inclusion of previously unconnected devices in the provision of data-driven services. Connected devices may be sensed and eventually manipulated remotely. Data obtained on a connected device may be forwarded, collected, aggregated and analysed. Data may be transformed, and data may be sent to a connected device, possibly triggering an action on the connected device.

The IoT is seen as an enabler for providing innovative services on the basis of smart infrastructure. Prominent examples include assisted living and smart home scenarios that aim for higher quality of living and efficiency gains alike. Similarly, smart city scenarios aim for sustainability and co-existence in our society by allocating resources efficiently.

On the other hand, ubiquitous digitisation gives rise to the question of whether the assessment of personal data and privacy outlined in the main body of this study may be expected to remain valid in the IoT, and where our expectations potentially lead to adjusted conclusions. On the one hand, we realise that data flows in the IoT are not fundamentally different from the data flows observed in any connected environment. This is due to the fact that the IoT is not fundamentally different by itself (devices have been connected before). It is the expression of digitisation that has been ongoing for quite a while but is intensifying in the IoT as it reaches more and more areas of life. On the other hand, the IoT shows a number of key characteristics providing grounds to anticipate adjusted conclusions:

- The IoT as a multiplier – an increased number of connected devices facilitates multiples of data to be produced and harvested: in the abundance of IoT market forecasts available today, specific figures on connected devices and numbers of transactions might differ. There is, however, consensus in terms of immense growth[212] being projected. This is further substantiated by various sector-specific analyses and forecasts. In light of the fact that Gartner currently positions IoT at the peak of inflated expectations[213], it is likely that the more optimistic forecasts may not come true. Whether solutions for items such as smart homes, assisted living or connected cars will be widespread according to any specific forecast does not matter that much; it is more important to realise

212 For instance, a recent Ofcom-commissioned study gives an impression of key market dimensions. More than 40 million IoT devices are currently deployed in the UK. This number is expected to grow by a factor of eight until 2022 resulting in more than 360 million IoT devices by then. See: Ægis (2014): M2M application characteristics and their implications for spectrum. Final report, 2606/OM2M/FR/V2: 1-78. Available at: http://stakeholders.ofcom.org.uk/binaries/research/technology-research/2014/M2M_FinalReportApril2014.pdf

213 Gartner (2014): Gartner's 2014 Hype Cycle for Emerging Technologies Maps the Journey to Digital Business. Press release. Available at: http://www.gartner.com/newsroom/id/2819918

that all signs point to digitisation further progressing, and progressing faster than ever. Irrespective of some setbacks such as the untimely launch of Google Glass as a premature consumer product,[214] one does not need to be a fortune teller to assume that the IoT will prosper. Many new devices have already been connected and lots more will follow. The sheer number of the connected devices will act as a multiplier for the respective data flows[215] from and to these devices and the services provided on top. In effect, more devices will have the potential to record and transmit personal data.

- The IoT as a diversifier – various types of connected devices facilitate richer data-driven services and near-seamless profiling: not only will many more devices be connected in the IoT, but the IoT will connect many different device types, ranging from tiny resource-limited sensors up to fully autonomous production plants. The IoT will be heavily heterogeneous, device-wise. Different devices mean specific capabilities and requirements. This will determine the set of supported data-driven services. It will also shape the ways in which humans and machines are able to interface and to interact. In effect, as the IoT will embrace more and more areas of consumers' lives as a result of the respective connected devices and services, there will be a substantially increased potential for data-driven services to broaden the coverage of data collection, to aggregate data from diverse sources and to base any sort of data analytics on a significantly richer data basis. Extended coverage also exposes the potential for comprehensive profiling across consumers' different whereabouts and activities throughout the day.

- The IoT as a decoupler – automated machine-to-machine communication leads to frequent data flows out of consumers' sight and control: machine-to-machine is the underlying communications principle for many IoT device types, for example in a connected car environment. The resulting data flows take place if certain contextual conditions are met or are at regular intervals. They are automated, which means they are not initiated by a consumer, at least not directly. Such data flows exist today, also on connected devices that are seemingly under user control when it comes to data communication. For instance, smartphones may track and transmit the location of the device in a fully automated fashion at regular intervals. As such data flows take place in the background, not requiring any user interaction or attention, it appears

214 Waters, R.; Bradshaw, T. (2015): Google suspends sale of smartglasses. Available at: http://www.ft.com/cms/s/0/ff12af46-9ce8-11e4-adf3-00144feabdc0.html

215 A recent Federal Trade Commission staff report on the IoT notes on the topic of privacy risks in the IoT that "[t]he sheer volume of data that even a small number of devices can generate is stunning: one [workshop] participant indicated that fewer than 10,000 households using the company's IoT home-automation product can "generate 150 million discrete data points a day" or approximately one data point every six seconds for each household." See: Federal Trade Commission (2015): Internet of Things. Privacy & Security in a Connected World. FTC Staff Report: 14.

reasonable to assume that this type of communication happens unconsciously. The consumer may have given consent to it, but this may be a long time ago and s/he will not be informed about it any further. The likelihood that a consumer loses track of automated data flows running in the background on the connected devices s/he actively uses is high. It is higher when considering connected devices that a consumer does not actively interact with. In effect, in the IoT, consumers may be consciously decoupled from both device and data flows.

The present study has established the status quo with respect to personal data and privacy, in particular with respect to informed consent in theory and practice. It found that consumers by and large do not read terms and conditions, that they do not understand them and that they do not act upon reading. The IoT characteristics described in the above indicate that the IoT will not only bring many more connected devices and even more data, but also different kinds of data covering more areas of life, and much of the communication will be decoupled from consumers. The following analysis thus looks at the main arguments encountered for which consumers do not read, comprehend or act, and it reasons whether these arguments need adjustment in an IoT context.

Argument	Reason
Consumers sign all sorts of contracts without reading them (clicking-without-reading phenomenon)	Due to high opportunity costs (not enough time to read all of it)

There is no reason to indicate that the clicking-without-reading phenomenon would go away with more and more previously unconnected devices becoming connected. The contrary effect seems more likely, namely that the IoT will aggravate the phenomenon. IoT will bring more and different newly connected devices, which sense, transfer and possibly analyse data that was not available before. Privacy policies will become longer as they will have to cover additional data and additional data uses. Longer privacy policies imply an increase in opportunity costs. It may even be that newly connected devices require new (additional) contracts to be established, in which case it is probable to assume that additional contracts come with a privacy policy of their own. The IoT may thus become a multiplier for contractual relations and terms and conditions. More contracts result in higher opportunity costs.

Argument	Reason
It is significantly easier for consumers to ignore terms and conditions in the data-driven environment	Unlike other purchases, there is no one to point consumers to terms and conditions and no physical signature is needed

By definition, the IoT implies the involvement of some sort of connected device in a data flow. Consumers will have to purchase (or possibly rent) such a connected device, or they will have to sign up for a service that includes the use of a connected device. Whether at that moment there will be someone to advise a consumer of the terms and conditions will depend essentially on the channel through which the respective connected device is sold. In case of a health monitoring device sold in a pharmacy, we may assume that pharmacy staff are trained to provide extensive advice prior to purchase. Pharmacy staff may in addition be aware of the sensitivity of health-related data. In contrast, a Nest thermostat purchased online for installation by the consumer[216] may replicate the problem that consumers easily ignore terms and conditions. Since the IoT will involve additional connected devices, out of which at least some risk replicating the problem, the problem will become more prevalent overall.

Argument	Reason
There is little if any incentive for consumers to engage with privacy policies	Reading data privacy policies would in many cases require more time than actually using a service

The use of connected devices in the IoT may be short term in certain cases. The majority of cases, however, will be longer term. Sensors and actuators in a smart home environment will be deployed for months and years. Devices like Google Glass or a smart watch will exhibit product life cycles similar to those of other mobile devices. The IoT is nonetheless expected to aggravate the above problem, albeit not for the reason of short usage times. The same effect may result from device separation (decoupling device from user). Many connected devices in the IoT will implement machine-to-machine communication. There will not necessarily be any direct human–machine interface. And even if there is, such as in the case of a connected pulse sensor, this interface might not support the device in showing a privacy policy to a consumer. As a result, consumers would have to read and accept the respective privacy policies on another device with a large enough display. This adds a hurdle to consumers actually reading privacy policies. Knowing that consumers have very little incentive to engage with privacy policies as it is, it is possible to conclude that adding a hurdle will not lead to more people reading privacy policies.

216 Nest (2015): Install it yourself. Available at: https://nest.com/thermostat/installation/#thermostat-diy-installation

Argument	Reason
There is little awareness among consumers about targeted advertising practices and what happens with their personal data when they surf the web or use a mobile app	Due to strong information asymmetry in the market

The information asymmetry consumers are exposed to today is likely to become more pronounced in the IoT. All of the three IoT key characteristics set out above have the potential to increase any existing differences in consumers' and providers' awareness of personal data uses, including targeted advertising practices. Consumers will have difficulties keeping an overview of many more connected devices in their surroundings and the data flows these devices initiate. With every data flow added, complexity for consumers to anticipate potential data flows and uses grows. Adding a single data flow means disproportional growth in combination options with available data flows. Consumers will be very likely to lose any ability to assess possibilities for data uses in the IoT. Keeping an overview will be even more challenging when the IoT reaches more areas of consumers' lives and allows a location- and time-wise near-constant tracking. And finally, the decoupling of users from devices by means of automated machine-to-machine communications will further any existing information asymmetry as consumers will be more likely to forget about the connected devices' very existence.

Aside from these risks of consumers losing track and control, consumers may be exposed in the IoT to additional issues emerging from information asymmetry. Take the example of a smart fridge. If the consumer opted for a smart fridge especially for the advantages it brings over a non-connected fridge, we may assume that the consumer made the respective purchase decision willingly and knowingly. If the consumer read, actually understood and accepted the according privacy policy, we may in addition assume the consumer gave his/her informed consent – informed consent to the data uses related to the functionality the smart fridge offers. However, it remains highly doubtful whether we could assume a consumer effectively grasped the consequences that arise from combining data flows from various connected devices, not just the smart fridge, for instance for purposes of personal profiling and targeted advertising. As a consequence, as long as there is information asymmetry regarding the full scope of possible data uses, our assumption on actual informed consent remains limited. The IoT's inherent complexity will aggravate this issue rather than help diminish information asymmetry.

Argument	Reason
Consumers do not understand the content of privacy policies	Privacy policies are cumbersome, poorly written and difficult to understand mainly due to the legalistic jargon they use

As we can anticipate the IoT to result in extended existing privacy policies and in more privacy policies overall, the problems consumers have today in understanding the content of privacy policies will prevail. The solution to these problems is to write privacy policies that are more accessible to consumers. Whether this issue may be successfully addressed or not depends on the privacy policies, not primarily on how many connected devices and data flows there are in the IoT. Connected devices are per se not to be blamed; rather, authors of privacy policies are. As we established that the complexity increase with any added data flow will grow disproportionately, it will be ever-more challenging to write a privacy policy that will allow consumers to understand what happens or may happen with their data.

In this respect, it is important to consider Nissenbaum's transparency paradox. For a privacy policy to be transparent, the privacy policy needs to point out exactly who interacts with the data, when, how and to what end. This objective conflicts with the objective to write easy-to-understand policies, especially in an IoT context with largely increased combination options for the many more data flows becoming available. Pointing out all possible interactions appears challenging at best and detrimental to consumers' understanding at worst. It will most certainly not lead to a policy that consumers have a good chance of understanding.

Argument	Reason
Consumers' scope to act is very limited	• Due to "take it or leave it" policies • Due to sophisticated tracking technologies, which are very difficult for consumers to evade • Due to consumers' limited willingness to pay for privacy as they cannot recognise quality (here, the absence of data collection for advertising)

Similar to the previous issue, the solution to consumers' limited scope to act depends on the nature of privacy policies and the tracking practices in use, not on the IoT per se. However, the situation in the IoT is expected to further strengthen the problem. There is no reason to believe privacy policies in the IoT will deviate from the current practice of issuing "take it or leave it" policies. In the same way, the same incentives that led to widespread use of advanced tracking technologies will prevail in the IoT. Finally, more connected devices will not give consumers any better way to recognise the value of privacy; the contrary might be more likely as we would expect the IoT to lead to a further increase in information asymmetry and complexity for consumers to assess what happens with their data.

7 Annex: Methodology

The literature reviews conducted for this study adhered to the typical quality criteria accepted in scientific writing. It has been ensured that there has been no personal bias. We were able to ensure this by internal review within the team and an additional external review by Dr. Aleecia M. McDonald. Throughout the process, attention was given to accurate use of the terminology in the area. To make the study more approachable for all readers, a glossary with the most relevant terms has been inserted at the back. An accurate and consistent referencing style has been used throughout the proposed study. Finally, a clear search and selection strategy that is a key precursor for a successful literature review has been used. The research objective for the proposed project naturally guided these search and selection criteria.

The search and selection criteria reflected the structure and overarching research question of the study. The studies were drawn from an extensive search of resources using specialized search engines such as Google Scholar and the search engines of scientific journal publishers. Naturally, our literature review cannot be fully exhaustive. We selected the papers based on their relevance for the research question as well as their date of publication. Generally, wherever possible we preferred more recent papers and papers that featured experiments with consumers. Other papers detailing for instance the strategies employed by governments to improve readership, understanding and consumers' action were selected to highlight also the effect that insights from behavioural economics already have had. As this literature review has shown, a quite substantial number of papers following an experimental approach exist. However, as the specific approaches and research objectives of the analysed papers differ quite substantially, a systematic literature review was not an option.

For each paper that featured an experiment or description of governmental action with immediate relevance to the research question addressed in this study, a short description was inserted into the annex to the study. Thus, the reader may refer to this description to find more detailed information on the methods, research objectives and results of the most relevant studies that have been cited in the study.

8 Annex: Studies

2000

Title	
When Choice is Demotivating: Can One Desire Too Much of a Good Thing?	
published in Journal of Personality and Social Psychology, Vol. 79, No. 6 pp. 995 -1006	
Year 2000	Authors Sheena S. Iyengar, Mark R. Lepper

Setting of the experiment

Study 1

"In this first field experiment, consumers shopping at an upscale grocery store encountered a tasting booth that displayed either a limited (6) or an extensive (24) selection of different flavors of jam. The two dependent measures of customers' motivation were their initial attraction to the tasting booth and their subsequent purchasing behavior."

"Over the course of [...] two 5-hr experimental periods, the behavior of approximately 754 shoppers was observed. Among the 386 customers present in the store during the hours when the extensive-choice booth was displayed, only 242 actually encountered the display. Among the 368 customers present in the store during the hours when the limited-choice booth was displayed, only 260 actually encountered the display."

"Two research assistants, dressed as store employees, invited passing customers to 'come try our Wilkin and Sons jams'. Shoppers encountered one of two displays. On the table were either 6 (limited-choice condition) or 24 (extensive-choice condition) different jams. […] Consumers were allowed to taste as many jams as they wished. All consumers who approached the table received a coupon for a $ 1-discount off the purchase of any Wilkin & Sons jam. Afterwards, any shoppers who wished to purchase the jam needed to go to the relevant jam shelf, select the jam of their choice, and then purchase the item at the store's main cash registers. As a result, regardless of the tasting-booth display encountered by each customer, all potential buyers of Wilkin & Sons products necessarily encountered the entire display of flavors."

Study 2

"Students in an introductory social psychology class were given the opportunity to write a two-page essay as an extra-credit assignment. Students were given either 6 or 30 potential essay topics on which they could choose to write. Intrinsic motivation was assessed by comparing the percentage of students who completed the assignment across the two conditions and the quality of the essays written in each condition."

"One hundred ninety-seven students in an introductory social psychology class at Stanford University served as the participants in this study. […] two separate sections, one of these two sections was assigned to the limited-choice condition and the other was assigned to the extensive-choice condition. [...] As a result, 70 students were assigned to the limited choice condition, whereas 123 students were assigned to the extensive choice condition." Study 3 "Participants initially made a selection from either a limited array or an extensive array of chocolates. Subsequently, participants in the experimental groups sampled the chocolate of their choosing, whereas participants in the control group sampled a chocolate that was chosen for them. Participants' initial satisfaction with the choosing process, their expectations concerning the choices they had made, their subsequent satisfaction with their sampled chocolates, and their later purchasing behavior served as the four main dependent measures in this study." "Conceptually, the design of Study 3 involved three groups: limited choice, extensive choice, and a no-choice control condition. [...]" Participants: "One hundred thirty-four students from Columbia University were randomly assigned to one of three conditions." Participants "sit at a round table on which there was one of two different displays of chocolates. In the limited-choice display, participants encountered one row of 6 different flavors of Godiva chocolates; in the extensive-choice display, participants encountered 30 different chocolates, arranged in five rows of 6." "In the payment room, a second experimenter, unaware of the condition assignments, greeted the participants. This experimenter offered the subject a choice of receiving a payment of either 5 dollars or a box containing four Godiva chocolates ordinarily priced at 5 dollars."
Research question Depiction of 3 experimental studies which are challenging/confounding the "assumption that having more choices is necessarily more intrinsically motivating than having fewer." "The three studies presented in this article […] examine for the first time the possibility that there may be differential motivational consequences of encountering contexts that offer a limited (i.e., psychologically manageable), versus an extensive (i.e., psychologically excessive), number of choices."
Results *(copied from abstract/conclusions of the publication)* "Findings from 3 experimental studies starkly challenge [the] implicit assumption that having more choices is necessarily more intrinsically motivating than having fewer. These experiments, which were conducted in both field and laboratory settings, show that people are more likely to purchase gourmet jams or chocolates or to undertake optional class essay assignments when offered a limited array of 6 choices rather than

a more extensive array of 24 or 30 choices. Moreover, participants actually reported greater subsequent satisfaction with their selections and wrote better essays when their original set of options had been limited."

Results 1

"Of the 242 customers who passed the extensive selection display of jams, 60% (145) actually stopped at the booth. In contrast, of the 260 customers who passed the limited-selection display of jams, only 40% (104) stopped. Thus, consumers who encountered the extensive-choice condition were more attracted to the booth than consumers exposed to the limited-choice condition". However, "nearly 30% (31) of the consumers in the limited-choice condition subsequently purchased ajar of Wilkin & Sons am; in contrast, only 3% (4) of the consumers in the extensive-choice condition did so […]."

Results 2

"Overall, 65% (126) of the students chose to do the assignment. There was, however, a significant effect of condition […]. Of the 70 students assigned to the limited-choice condition, 74% turned in the assignment. In contrast, of the 123 students assigned to the extensive-choice condition, only 60% chose to complete the assignment. […]For content, […] on average, students assigned to the limited-choice condition performed slightly, although significantly, better […] than those assigned to the extensive-choice condition […]. A similar main effect was found for form […]. On average, students in the limited-choice condition scored higher […] than students in the extensive-choice condition […]."

Result 3

"[…] participants spent significantly more time (in seconds) deciding which chocolate to sample when there were 30 chocolates […] than they did when there were only six […]."

Moreover, the "participants' responses to the question concerning whether they felt the number of choices available was too few, just right, or too many. Here again, there was a significant effect for the number of options presented […]. Participants who encountered 30 chocolates reported feeling that they had been given "too many" […], whereas participants who encountered 6 chocolates reported feeling that the number of alternatives was "about right" […]. These data provide direct evidence for [the] assumption that 30 chocolates would seem an overly extensive choice set."

The "participants offered extensive choices […] also reported finding the decision-making process to be more difficult than did participants offered more limited choices […]."

"Participants in the limited choice condition (48%) were significantly more likely to choose chocolates as compensation, as compared with participants in both the extensive-choice condition (12%) […] and the no-choice condition." The Participants in both the extensive-choice condition and the no-choice condition choose money as compensation.

General results

“Studies 1, 2, and 3 provide compelling empirical evidence that the provision of extensive choices, though initially appealing to choice-makers, may nonetheless undermine choosers' subsequent satisfaction and motivation.”

The authors found “considerable empirical support for the theory that choosers in extensive-choice contexts enjoy the choice-making process more — presumably because of the opportunities it affords — but also feel more responsible for the choices they make, resulting in frustration with the choice-making process and dissatisfaction with their choices.”

2004

Title International Differences in Information Privacy Concerns: A Global Survey of Consumers	
published in The Information Society, 20: 313–324.	
Year 2004	Authors Steven Bellman, Eric J. Johnson, Stephen J. Kobrin, Gerald L. Lohse

Setting of the experiment

Bellman et al. used a "sample of Internet users from 38 countries" and matched them "against the Internet population of the United States".

The final sample "consisted of 534 valid responses from 38 countries. Less than half of the participants (37%) were females, the mean age was 32.7 years, the mean education level was 4.5 (between "some college" and "college graduate"), and the mean level of Internet experience was 27 months. Only 23% were fulltime students. The U.S sample contained was slightly more educated, compared to U.S. panelists in general (who were representative of the U.S. Internet population), but had identical levels of privacy concern. U.S. panelists, both participants in the survey and nonparticipants, had the same level of concern about third parties monitoring their online transactions, and were equally likely to give their name, e-mail address, and telephone number to a Web site. Compared to the U.S. participants, International participants had identical Internet experience and demographics, with the exception of being slightly younger."

Survey Items

- Concern for Information Privacy can be summarized into four categories: collection, unauthorized secondary use, improper access, and errors. A "Seven-point Likert scales (1 = "strongly disagree" to 7 = "strongly agree") were used with a "no opinion" option so that responses were not forced.
- Concern about Transaction Security on the Internet
- Desire for More Regulation
- Information Privacy Regulatory Approaches

Bellman et al. "used a multivariate analysis of covariance (MANCOVA) to test the significance of the independent variables – cultural values, regulatory structure (no regulation, sectoral, and omnibus), and Internet experience – on a set of dependent variables examining privacy and security concerns, and desire for more privacy regulation. The covariates controlled for demographics (age, gender, and level of education) and order of presentation (privacy scale items first or questions about the need for more regulation first) in every analysis.

Hypothesis:

- H1: Cultural values will be associated with differences in concerns about information privacy.
- H2: Consumers from countries with an omnibus privacy regulatory structure will have higher levels of privacy concerns compared to consumers from countries with sectoral privacy regulation or no privacy regulation.
- H3: Higher levels of current government involvement in the regulation of corporate privacy management will be associated with a greater preference for even stronger laws to regulate information privacy.
- H4: Participants with more Internet experience will exhibit lower levels of concern about the privacy of their personal information.

Research question

Examination of “three possible explanations for differences in Internet privacy concerns revealed by national regulation: (1) These differences reflect and are related to differences in cultural values described by other research; (2) these differences reflect differences in Internet experience; or (3) they reflect differences in the desires of political institutions without reflecting underlying differences in privacy preferences.”

Results

(copied from abstract/conclusions of the publication)

They “found significant multivariate effects for regulatory structure and Internet experience, providing support for H3 and H4, but not for H2. We did not find consistent support for H1, the effect of cultural values.” In their sample, “the influence of cultural values was only seen in two dimensions of information privacy concerns, errors in databases and unauthorized secondary use, rather than in overall concern for information privacy.” Nevertheless, “cultural values do have an influence on consumers’ concerns about information privacy” to a certain extent.

As mentioned above they found support for their hypotheses “about the influence of national regulation on privacy concerns. Consumers from countries with a history of introducing government regulation of information privacy desired even stronger regulation of data collection […]. But, they also found “that consumers from countries with no privacy regulation were more concerned about one aspect of online privacy, errors in databases, than consumers from countries with sectoral privacy regulation. Consumers from countries without privacy regulation were also more concerned about the security of online transactions than consumers from countries with any form of privacy regulation, either sectoral or omnibus.”

One important finding in this study “is that privacy regulation mediates cultural differences in information privacy concern. However, while including regulation in a model absorbs many of the effects of culture on privacy concerns, particularly those about errors in databases, other concerns surface that were previously obscured. These concerns about improper access and unauthorized secondary use […] and about

the security of online transactions […] are likely to persist, even if country differences in regulatory regimes were harmonized." Finally, the authors "found consistent evidence that online privacy concerns diminish with Internet experience."

Title An Imbalance Of Power: The Readability Of Internet Privacy Policies	
published in Journal of Business & Economics Research, Volume 2, Number 3	
Year 2004	Authors Rochelle A. Cadogan
Setting of the experiment „This research project is a multiple case study in which the privacy policies of three organizations are evaluated in terms of their readability and their user-friendliness. The three online organizations selected include PrivacyAlliance.org, Dell.com, and Amazon.com. [...] A review of those documents by the researcher will be a primary source of data. Consumer evaluations (done by adult students, age 25 or older, as a class project), interviews, writing analysis tools, and electronic communication have been utilized in this research investigation."	
Research question How understandable are internet privacy policies?	
Results *(copied from abstract/conclusions of the publication)* "The Online Privacy Alliance policy is very brief and concise. The policy is generally easy to read and understand. The students who evaluated the policy felt that the public would not have a problem understanding the policy. One comment made by a participant in the study was that after reading this privacy policy, the other policies previously read seem much more confusing." "The students who evaluated the policy [of Dell] generally believed that the policy is written at high school level or slightly higher. Some of the terminology regarding computer technology such as data —encryption‖ and —cookies‖ may be unclear to many readers but the privacy policy provides links to clarify meaning of many of the statements that may be unclear. Evaluators found this descriptive and explanatory content very beneficial." Some evaluators believed that language in the [Amazon] policy, for the most part, is no higher than a high school difficulty level and some statements regarding computer technology may be unclear at that level. Consumer rights are adequate and expressed in a straightforward manner with the exception of sharing information with other third parties. Some evaluators felt that Amazon.com was very thorough in explaining how and what	

information is collected from the customer and the content of the policy was clear. [...) The —opt-outǁ option received some criticism by the evaluators. Some evaluators felt that it was difficult, or even impossible, to —opt-outǁ at the Amazon.com site.

The author comes to the overall conclusion that “Internet consumers are facing an increasingly hostile environment. Faced by online profiling companies that seek to know about their online surfing habits and Web sites that change their privacy policies at will, consumers are increasingly left to their own devices in protecting their privacy. [...]

As a safeguard, the consumer should look for a privacy policy on the Web site before making a purchase online. Unfortunately, for the organization, just having a policy on the site is not enough, which this study verifies. Privacy policies vary widely in the information they provide to the customer and the manner in which the information is presented. The privacy policy represents important legal information and should be given significant attention in designing an online environment for any organization. Companies should provide consumers with notices that are easy to locate, read, and understand. These notices should clearly state the company's information collection and sharing practices and provide customers with choices regarding these practices. [...]

The technology sector must do a better job of educating and empowering consumers so they can feel safe on the Internet and so legislators will be less inclined to overact and legislate quickly without taking stock of all the consequences of a regulated Internet. The bottom line is that the privacy policy of any organization must be understandable and there is room for improvement.“

Title
Was Verbraucher wissen wollen. Ergebnisse und Thesen zu einer empirischen Studie [What consumers want to know. Results and hypothesis to an empirical study]
published in
Vortrag von Ingo Schoenheit zu: Schoenheit, I. (2004): Was Verbraucher wissen wollen. Empirische Studie zum Informationsbedarf der Verbraucher. Verbraucherzentrale Bundesverband e.V. (Hrsg.), Berlin 2004

Year	Authors
2004	Ingo Schoenheit, imug - Institut für Markt-Umwelt-Gesellschaft e.V.

Setting of the experiment
Representative study of adult population in Germany (N = 1,000). Survey via telephone interviews.
Respondents were asked about how many and which information they need about consumer products (food, textiles, automobiles, electric power, pension schemes).

Research question
Which kind of information do consumers need? How much? Provided by whom? Which kinds of legal information requirements are useful and which ones are obsolete from the consumer's point of view?
Results
(copied from abstract/conclusions of the publication) Schoenheit found out that apparently consumers use only very few legally required information offers. For example, when buying food, only 2% of the adult population actually read the list of additives on the product. However, there was no evidence found that they would like to renounce any information. The more important the quality of the product is to the consumers the more unsatisfied they seem to be with the information standard provided.

Title	
Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices	
published in Journal of Interactive Marketing, Vol. 18, No. 3, pp. 15-29.	
Year 2004	Authors George R. Milne and Mary J. Culnan
Setting of the experiment "The research was conducted as a field study. […] Harris Interactive administered the final survey and collected data online form November 6-8, 2001. A stratified random sample of 2,468 U.S. adults was drawn from the multi-million member Harris Poll Online panel based upon known proportions of age, gender, and region in the U.S. population." "Survey respondents were asked how frequently they read privacy notices posted by Web sites using a five-point scale ranging from 1=never read them to 5= always read them." In testing their hypotheses, they "excluded non-readers"	
Research question "This study examined reasons and situations when consumers read privacy notices and where they use alternatives for privacy notices."	
Results "For the respondents who read privacy notices, control over personal information emerged in the open-ended comments as a main reason for reading the notices, especially when consumers were asked to disclose sensitive information. […] Others read notices to see how their personal information would be used, particularly if it would be shared with other organizations […]. Still others felt that there was no risk-based	

reason to read notices. While privacy concern remains a big motivator for consumers to read notices, the study also found that perceived comprehension of notices also had a strong effect. If the notice is not perceived as comprehensible, then it will be less likely to be read. […] Alternatively, when consumers perceive they can comprehend privacy notices, the more likely they are to both read notices across an array of situations and to trust the notices. Further, some of the comments also suggested that notices that are perceived by consumers to be obfuscated or excessively legalistic can contribute to scepticism […]."

Moreover, if "consumers perceive privacy notices as being irrelevant because of format issues, they may balk at even attempting to read them […]."

2005

Title Privacy practices of Internet users: Self-reports versus observed behavior	
published in Int. J. Human-Computer Studies 63 (2005): 203–227	
Year 2005	Authors Carlos Jensena, Colin Pottsa, Christian Jensen
Setting of the experiment The 175 volunteer subjects “came from diverse backgrounds, though approximately two thirds were currently involved in education (students, faculty and researchers). [...] Subjects were anonymous; [...] The study was divided into four separate but interrelated sections: (1) A basic demographic survey. (2) A survey of privacy values and attitudes. (3) A set of questions challenging users’ knowledge of specific technologies and how they affect privacy. (4) An experiment presenting subjects with a series of pair-wise comparison tasks to determine the effect privacy indicators have on actual behavior.” <u>Privacy values:</u> This section of the survey was used to divide the subject into 3 categories. Subjects are categorized based on their answers to “five questions: 1. I am concerned about online identity theft. 2. I am concerned about my privacy online. 3. I am concerned about my privacy in everyday life. 4. I am likely to read the privacy policy of an ecommerce site before buying anything. 5. Privacy policies accurately reflect what companies do.” The authors “classified a participant as a ‘Fundamentalist’ if he or she gave a privacy-oriented response to four of these five questions (and no negative answers). A participant was classified as ‘Unconcerned’ if he or she gave no privacy-oriented responses (and at most one neutral response) to these five questions. The remaining participants were classified as Pragmatists. […]. “ Results: Fundamentalist 34%, Pragmatist 43%, Unconcerned 23%.	
Research question Examination of “visible indicators of privacy invasions or privacy guarantees” which “are effective in swaying consumers’ purchase decisions.” The authors also examine “what effects gender, level of experience, and other demographic variables have on reported and observed behavior.” Finally, they “investigated the salience of categorization schemes for users privacy concerns based on survey responses.”	

Results
(copied from abstract/conclusions of the publication) "This paper reports on a study in which (1) user concerns [about privacy] were analysed more deeply and (2) what users said was contrasted with what they did in an experimental e-commerce scenario. Eleven independent variables were shown to affect the online behavior of at least some groups of users. Most significant were trust marks present on web pages and the existence of a privacy policy, though users seldom consulted the policy when one existed." The authors also "find that many users have inaccurate perceptions of their own knowledge about privacy technology and vulnerabilities, and that important user groups […] do not appear to form a cohesive group for privacy-related decision making."

Title	
Privacy and Rationality in Individual Decision Making	
published in IEEE Security & Privacy Vol. 3, No. 1, January/February 2005, pp. 26-33	
Year 2005	Authors Alessandro Acquisti, Jens Grossklags
Setting of the experiment The authors conducted an online, anonymous survey about e-commerce preferences in 2004. "The survey contained several questions organized around various categories: demographics, a set of behavioral economic characteristics (such as risk and discount attitudes), past behavior with respect to protection or release of personal information, knowledge of privacy risks and protection against them, and attitudes towards privacy [...]."	
Research question Investigation of "the drivers and apparent inconsistencies of privacy decision making" and testing "the rationality assumption by analyzing individual knowledge, behavior, and psychological deviations from rationality in privacy-sensitive scenarios."	
Results *(copied from abstract/conclusions of the publication)* The author detected that "individuals make privacy-sensitive decisions based on multiple factors, including (but not limited to) what they know, how much they care, and how costly and effective their actions they believe can be." Although the participants "displayed sophisticated privacy attitudes and a certain level of privacy-consistent behavior, their decision process seems affected by incomplete information, bounded rationality and systematic psychological deviations from rationality." So, "even if	

individuals have access to complete information about their privacy risk and modes of protection, they might not be able to complete information about their privacy risks and modes of protection, they might not be able to process vast amounts of data to formulate a rational privacy-sensitive decision. Human being's rationality is bounded, which limits out ability to acquire and then apply information. [..] Even individuals who claim to be very concerned about their privacy do not necessarily take steps to become informed about privacy risks when information is available. […] Even with access to information and unbounded ability to process it, human beings are subject to numerous psychological deviations from rationality than a vast body of economic and psychological literature has highlighted: from hyperbolic discounting to underinsurance, optimism bias and others."

Title	
Open to Exploitation: American Shoppers Online and Offline	
published in Annenberg Public Policy Center report, June 2005	
Year 2005	Authors Lauren Feldman, Joseph Turow and Kimberly Meltzer
Setting of the experiment Prices that vary based on firms' information about consumers is becoming an increasing feature of the marketplace. In particular, there are two main developments: "behavioral targeting and price discrimination. Behavioral targeting in a retail environment takes place when a firm keeps track of a customer's shopping history in order to know how to best sell to him or her. Price discrimination comes in a variety of forms, economists note. The ones that most attract retailers involves using information to change prices based on what the seller knows about individual consumers or consumer segments." Regarding this new developments, the authors "asked a nationally representative sample of 1,500 adults who used the internet during the past month 17 true-false questions about key aspects of these new developments and where they can turn for help if their personal information is used illegally." Because their "questions relate to both the online and offline marketplace" they "focus on U.S. adults who use the internet." They included people who were 18 years old or older. Their "questions aimed to focus on two areas. One was people's knowledge of the law when it comes to a company's right to collect information about them online or offline and to charge them and others different prices for the same items at the same time. The second area centered on people's attitudes regarding these activities." The interview schedule had seven parts. "Part 1 asked about the person's internet use. Part 2	

solicited people's views about companies' having access to their personal information, profiling them behaviorally, and charging them different prices—sometimes to their benefit—based on what they learn. In Part 3 the interviewee was given a series of statements about the rules of price discrimination and profiling—especially behavioral targeting—in the marketplace and asked whether each was true or false. Part 4 involved three short scenarios describing different types of behavioral targeting and soliciting the person's opinions about their ethical acceptability Part 5 asked people to agree or disagree about statements regarding privacy and personal information. Part 6 asked about the person's everyday privacy-protecting activities and concerns online and offline. And Part 7 requested background data such as age, education, and ethnicity." The telephone interviews took in average 20 minutes.

Research question

The authors conducted a national phone survey in the U.S. Their goal "was to generate a series of propositions about what consumers ought to know regarding three topics: who is allowed to control the profiling information about them that can lead to price discrimination, whether the law protects them from secret forms of price discrimination offline and online, and where they can turn for help if they worry that their information is being abused."

Results

The study reveals that:

1. "Most internet-using U.S. adults are aware that companies can follow their behavior online. Fully 80% know marketers "have the ability" to track them across the web, and 62% know that a company "can tell" if they have opened its email without getting their response.
2. "Large majorities of internet-using U.S. do not understand key laws and practices relating to profiling, behavioral targeting and price discrimination."

Just 50% of the "internet-using adults is aware of these realities means that the other 50% do not understand them. In this connection, the inability of half the respondents to discern phishing is particularly alarming because of the activity's growth. […] It is also troubling that around 50% of internet-using U.S. adults are unaware that information about them can move between magazines and amid affiliated websites without their approval. A similar percentage thinks they have more control over the information that online firms hold about them than they actually do. A far higher percentage - 75% - doesn't realize that that the mere presence of a privacy policy is no indication that a site will refrain from sharing visitors' information. This pattern of unawareness online and offline may well lead them to be less careful about providing certain sorts of information to merchants than they would be if they knew what actually takes place."

The study also indicates a "lack of knowledge about the legal right of supermarkets, video stores and charities to sell personal information; of banks to share customer information with affiliates; and of retailers' to discriminate on price. When it comes to these topics, from 63% to 72% of respondents are wrong. […] It might seem odd that

higher proportions of respondents are incorrect about the legality of information-sharing by banks, charities, supermarkets and video stores than by magazines and non-specific 'websites'.

The study also reveals that:

3. Large majorities of internet-using U.S. adults do not know basic places to turn for help if their marketplace information is used illegally. The lack of understanding regarding marketplace laws and practices carries over to their understanding of where they can go for recourse if things do go wrong.

Insights about price discrimination: "Evidence suggests that people don't expect that it is happening to them on a continual basis. Even though people know that they are tracked on the internet, only 21% agree that 'The information I give online stores about myself will often determine the prices they will charge me.' […] When presented […] various concatenations of price discrimination, between 64% and 91% of respondents registered aversion to the activity. Interestingly, a smaller percentage (64%) disagrees with discount coupons as mechanisms for price discrimination compared to simply asking for less money (76%). The largest percentages are riled about the idea of different people paying different prices for the same products during the same hour. 87% disagree with the implementation of such a practice by an 'online store' and 91% disagree with its taking place in the supermarket."

Insights about behavioral tracking: "45% of the respondents say that changing the ads based on what the site 'sees you reading on the site' is a good or very good idea; 22% think it is a bad or very bad idea, while 33% say it is neither good nor bad. By contrast, 46% of the respondents believe that from a consumer's standpoint it is a bad or very bad idea to change the products they see based on purchased personal information. 23% say it is a good or very good idea, and 29% say it is neither good nor bad."

In principle, the "findings suggest that most internet-using adult Americans will fall prey to marketplace manipulations even while many believe (incorrectly) that they know how to handle themselves. […] Consumers who are not aware of how price discrimination and behavioral targeting work, of what rights they hold when it comes to companies' using knowledge about them, and of how to respond to these circumstances may find themselves consistently paying more than others for the same products." Their "data indicate that overwhelming portions of internet-using adult Americans object to price discrimination that is guided by behavioral targeting." The "data also suggest they would be quite angry if they found out it is happening to them. Americans who suspect themselves disadvantaged as a result of these often-hidden activities (but don't know what to do about them) may well turn against the corporate and government institutions who they believe are encouraging the practices. That could ignite new marketplace tensions - and possibly even broader frictions - within U.S. society."

The authors, therefore, suggest three policy initiatives:

1. "The Federal Trade Commission should require websites to drop the label Privacy Policy and replace it with Using Your Information."

2. “U.S. school systems - from elementary through high school - must develop curricula that tightly integrate consumer education and media literacy.”
3. “The government should require retailers to disclose specifically what data they have collected about individual customers as well as when and how they use those data to influence interactions with them.”

2006

Title Evolution of a Prototype Financial Privacy Notice. A Report on the Form Development Project	
published in http://kleimann.com/ftcprivacy.pdf	
Year 2006	Authors Kleimann Communication Group, Inc.
Setting of the experiment Evolution of a Prototype Financial Privacy Notice: “The financial privacy notice prototype evolved in content and design based on an iterative process of consumer research, rigorous data collection, thorough analysis, and the expertise of the information designers and legal experts.” They use a “small numbers of participants to explore in a realistic manner how and why consumers understand and make sense of a document.” For the Form Development Project, they “used four qualitative methods - focus groups, preference testing, pretest, and diagnostic usability testing - to iteratively develop and refine the prototype according to the goals of comprehension, comparability, and compliance.” “The following five questions helped guide the development of the prototype content and design. How do we: 1. attract consumers’ attention to the notice using only objective and factual language; 2. decide what information to include; 3. ensure that consumers can understand about the sharing of their personal information; 4. ensure that consumers can compare sharing practices across financial institutions; and 5. enable consumers to understand how to opt out.”	
Research question Exploration of “the reasons why consumers don’t read and understand privacy notices” and Development of “alternative privacy notices – or components of notices – that consumers can understand and use.” They are trying to provide a “prototype” privacy notice.	

Results

(copied from abstract/conclusions of the publication)

Test results:

Focus Group: “The focus group results indicated that most participants don’t currently read the privacy notices they receive from their financial institutions. […] Some participants mistakenly thought they could opt out of all sharing types. Others were confused by their opt-out choices […]. Many failed to recognize there were opt-out options […] Participants also expressed concerns about notices that were too long and too time-consuming to read. At the same time, they wanted to make sure that they had complete information. Some suggested a shorter notice or notice summary accompanied by more detailed information—a type of layered notice. Most didn’t want to have to take an extra step and contact the bank for the additional details. They wanted to receive both concurrently. “

Preference testing: “The purpose of the preference testing was to collect baseline information on participants’ preferences and opinions on components. Since they were given only parts of the notice, it wasn’t expected that participants understand the purpose of and context around financial information sharing. Many preference questions yielded mixed responses with no clear preference for any one choice. Others indicated stronger tendencies.”

Pretest: “Participants didn’t understand the purpose, content, or opt-out information in any design or version. Although participants were able to find and recall information, their answers were not based on the information in the designs. Instead, participants tried to understand the information in the notices by applying anything they knew that was remotely related to banks, privacy, or their finances to figure out the information. Unfortunately, most of their applied knowledge was incorrect.”

Diagnostic usability testing: Different prototypes in different states were tested. “All in all, the prototype and its components were working in terms of comprehension, comparability, and compliance.”

Conclusion:

“The prototype has four key components – the title, the frame (key and secondary) the disclosure table, and the opt-out form.”

Title: “The title helps consumers understand that the notice ID from their bank and that their personal information is currently being collected and used by their bank.”

Frame: The frame “provides basic information about financial sharing practices as a context for consumers to understand the details of their particular bank’s sharing practices.”

Disclosure Table: The disclosure table “shows what the […] financial institution is sharing” and includes “basic reasons [why] any financial institution can share information”. It “enables consumers to understand the details of their financial institution’s sharing practices.

Opt-out Form: This form “identifies how a particular financial institution allows consumers to limit a particular type of sharing.

Meta-themes: The prototype developed by the authors is grounded in these themes:

1. “Keep it simple”: Their research “showed that consumers are overwhelmed by too many words, complex information, and vague words and phrases.” There have to be a balance between “as few words as possible an enough information so consumers understand” the information.
2. “Good design matters”: Their research showed “that consumers responded positively to […] table design[s], headings, white space, bold text, bulleted lists, a larger front size, and full-size paper.”
3. “Carful design decisions ensure neutrality”: Privacy notices “need to deliver information about financial sharing practices in a way that reports the information truthfully.”
4. “Standardization is highly effective”
5. “The disclosure table is critical”: “[…] standardized disclosure table simplifies highly complex and mandatory information into a design that consumers can understand without undue burden.”

2007

Title	
Warning: Too much information can harm. A final report by the Better Regulation Executive and National Consumer Council on maximising the positive impact of regulated information for consumers and markets.	
published in http://bre.berr.gov.uk/regulation/reform/next_steps/too_much/	
Year 2007	Authors Better Regulation Executive and National Consumer Council
Setting of the experiment The initiators received responses to the interim report from individuals, businesses, Third Sector organisations, Government and international contacts and conducted individual tests on: Test a: Behavioural outcomes Test b and c: Incentives for consumers and businesses Test d: Simplification Test e: Fit with existing requirements Test f: Alternative information approaches	
Research question „Maximising the positive impact of regulated information for consumers and markets"	
Results *(copied from abstract/conclusions of the publication)* From January to October 2007, the Better Regulation Executive and National Consumer Council conducted a review of the extent to which information was achieving its goals, based around focus group research with consumers and a series of stakeholder interviews. The research focused on 7 case-studies of regulated information, ranging from recycling symbols to product safety warnings on toasters. The research found many pieces of information were simply not having the impact on consumer behavior they set out to achieve. Consumers rejected much of the information because it was not helpful or was presented in a complex or unappealing format. Information requirements were also an irritant for business, due in large part to the complex systems companies have to put in place to ensure compliance. "In summary, our work found that although information can be a powerful tool it is neither failsafe nor costless. When presented to consumers, many of the pieces of information from our case studies were not having the desired outcomes. Consumers rejected much of the information because there was too much of it and because it was	

presented in a complex and unappealing format. Whether the 52 safety warnings on a toaster or the consumer credit agreement that required 55 minutes to read, consumers did not find the information being provided helpful. Some of the more vulnerable groups we spoke to found overly complex information not only difficult but also humiliating. Across society our research found a desire for simple, succinct information. Decision-trees and other tools that helped people navigate through the process of making choices were preferred to text which was often written by lawyers.

For business, the provision of information was an irritant, and often more than that. The volume of requirements means some businesses have to put in place monitoring systems to ensure compliance. For example one consumer credit provider ensures that all agreements are verified by eight different people before approval. It has to be expected that some of these costs are passed on to consumers, although there is no hard evidence of this. Information requirements are also an irritant to business where they cut across their other communications with consumers or constrain the extent to which they can tailor their messages."

Title	
Consumer Information Sharing: Where the Sun Still Don't Shine.	
published in	
University of California, Berkeley, December 17, 2007	
Year	Authors
2007	Chris J. Hoofnagle, Jennifer King

Setting of the experiment

"Students working the Samuelson Law, Technology & Public Policy Clinic during Summer 2007 each chose businesses with which they had a relationship to send SB 27 requests. Students chose companies that were not banks, and that appeared to have over 20 employees."

The authors chose the "following methods of contacting the business, in order form most preferable to least: a point of contact obtained from a "Your California Privacy Rights" webpage; one obtained from calling or mailing customer service; one obtained by visiting the business; one obtained from privacy policy page; one obtained from a webpage for legal matters; or one obtained from a general customer service webpage."

The "requests were sent on June 14, 2007. SB 27 requires a response to a request within 30 days. In order to account for mailing delays, [they] waited 40 days for responses. On day 41 (July 25, 2007), [they] sent replies to responses that were inadequate, and sent reminder letter to companies that did not respond at all."

Research question
Testing of the implementation of SB 27, the “Shine the Light Law”, “to better understand how businesses sell personal information, and to map the landscape of information sharing among different businesses.”
Results
“Of the 86 requests, two companies disclosed a list of information sharing partners. […] Twenty-two companies responded by providing a privacy and an opportunity for the individual to opt out. Forty-three companies responded by providing a privacy policy or letter that indicated that the company does not sell personal information to third parties without opt-in consent.” They “categorized nine responses as ‘other’, usually because the businesses claimed that the requestor had to prove that an established business relationship existed. Finally ten companies did not respond at all as of this writing.” “[…] companies that responded did so in 32.6 days […]. Several companies responded with 7 days.” Three of the companies “that did not respond within 40 days of the initial request had TRUSTe privacy seals on their websites. […] Since these three companies did not respond, the student wrote to TRUSTe to complain. TRUSTe opened case numbers for all three, and within a short time, all three companies responded.” “Privacy laws such as SB 27 are generally conceived of as a tool for consumers to expose business practices. But even companies that sell their consumer databases to third parties can write a response that places the company in a good light.” Furthermore, “privacy policies are so confusing that in some cases, our students did not fully understand the responses. For instance, if a company offered an ability to opt out of a newsletter, some students mistook this to mean that the company sold data to third parties, and was offering an opt out of information sharing.”

Title	
The Value of Privacy Assurance: An Exploratory Field Experiment.	
published in MIS Quarterly 2007 (31): 19-33.	
Year 2007	Authors Hui, K.L.; Teo, H.H. and Lee, S.Y.T.
Setting of the experiment The authors conducted an “exploratory doled experiment in Singapore.” They “used electronic mail to invite a group of subjects to visit [their] experimental website (which was hosted by a Singapore firm that specialized in market research) to fill out a survey about mobile computing products.” An e-Mail was sent by the firm in Singapore to “600 business students at a large Singapore university who had no previous transaction history with” them.”137 students	

visited the experimental website and, among them, 109 completed the experiment." These 109 subjects were on average 24 years old; "the age range was 21 to 28; with 53 percent of the sample being female."

They "also assigned a unique one-time access code to each invited subject to prevent repeated participation." At first, they "did not reveal the experiment to subjects, and [they] presented the three treatments – privacy assurance, monetary incentive, and information request – to subjects only after they entered a valid access code."

"The survey contained some mandatory information items that subjects were required to provide to complete their participation, and a set of optional questions about mobile computing products. The optional questions were included to disguise the study's purpose; answers to these questions were not uses in the analysis."

"Regardless of whether subjects completed the survey […], a follow-up survey was posed to elicit some necessary information including manipulation checks, past experiences, etc. To encourage subjects to do the follow-up survey," they gave them 20 Singapore dollars. "The follow-up survey required only 10 to 15 minutes of effort, and asked mostly for personal opinions."

The authors "created three scenarios for privacy assurance: (1) no assurance; (2) assurance by means of a privacy statement; and (3) assurance by means of both a privacy statement and privacy seal." The website of the firm in Singapore was certified by TRUSTEe, which "was among the most popular privacy seals used by online firms." These three treatments were randomly shown to the group of subjects. The experimental website was not just hosted under the firm's home page it also carried the firm's domain name. Furthermore, "only the firm (not the authors of this paper) interacted with the subjects."

They "further manipulated two factors in the experiment, monetary incentive and information request." "For the monetary incentives, once subjects arrived at the experimental website, [they] informed them that they would receive a check upon completing the (main) survey. The value of the check was not disclosed in the invitation, but was revealed only after subjects arrived at the website. It varied from 1 to 9 Singapore dollars […]. The check (and a separate check for 20 Singapore dollars if a subject also completed the follow-up survey) was mailed to each subject after the experiment by our partner firm." Then they also "manipulated the information requests by varying the number of mandatory items in the main survey. Each subject was asked to disclose between 4 and 23 pieces of personal information […]." They "ordered the items so that the longer treatments always encompassed the shorter ones. The base treatment asked for only name, e-mail, address, and citizenship. The next treatment added gender, then marital status, ethnicity, and so on. This helped ensure effective variation in information requests across subjects."

The collected additional data in the follow-up survey were used as control variables in the subsequent analysis. First, they "measured subjects' propensity to trust others with two 7-point Likert scale items (all Likert scale items in this study had the anchors 1 = totally disagree and 7 = totally agree)." Second, they "asked subjects whether they had

prior experience with personal information misuse." Finally, they "measured subjects' privacy concerns by two means."
Research question Assessment of the "values of two types of privacy assurance: privacy statements and privacy seals." Research questions: "Do consumers value privacy statements and privacy seals? If so, do these statements and seals affect consumer disclosure of personal information?"
Results The researchers found that: 1. "The existence of a privacy statement induced more people to disclose their personal information to a website. By contrast, presenting a TRUSTe privacy seal did not have any significant influence. These findings were robust regardless of whether or not the subjects had read and understood the purpose of the privacy statement and privacy seal." 2. "Monetary incentive had a positive influence on disclosure." 3. "The amount of information requested had a negative influence on disclosure: The more information requested, the less likely the subjects were to disclose it. The sensitivity of the information, however, had no significant influence." 4. "Results 1., 2., and 3. were robust across alternative specifications that used different measures for information sensitivity and privacy concern."

Title	
Promoting I-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behaviors	
published in Journal of Consumer Affairs, Vol. 41, Issue 1, pp. 127-149.	
Year 2007	Authors Robert Larose and Nora J. Rifon
Setting of the experiment "Two hundred and twenty-seven participants were recruited from undergraduate classes in advertising and agriculture at a major Midwestern University." "A 2x2 experimental design was created by manipulating the presence/absence of a privacy warning label, and the presence/absence of a privacy seal on a stimulus website. Data were collected in two, separate on-line sessions that respondents attended through their own personal computers. […] Privacy involvement was split at its median value of 8 to assign equal numbers of respondents to high and low involvement	

groups. Respondents were randomly assigned to one of four groups within each involvement level." "Four stimulus websites were created for a fictitious company, Amazingdeals.com. The stimulus websites contained Amazon.com's privacy policy statement from April, 2003. […]The 2x2 privacy warning label x seal manipulations were created using four conditions, one condition presented a privacy warning label and a privacy seal, one a privacy warning label but no seal, one without a privacy warning label and with a privacy seal, and one with neither a privacy warning nor privacy seal, thus creating the 2x2 warning x seal manipulations." Furthermore, a "privacy warning label was created to provide a clear and conspicuous presentation of the stimulus website's information practices, facilitate comprehension, and to minimize information overload presented by presently existing privacy policies."
Research question This "study experimentally examines the effects of explicit privacy warnings."
Results "When unambiguous information about potential negative outcomes of privacy disclosures was communicated to consumers it made them less inclined to supply personally identifying information and less likely to purchase products from Web sites that put their privacy at risk. However, consumers differ in their perceived abilities to protect themselves, their privacy self-efficacy beliefs, and this may be the key to unraveling the privacy paradox. While privacy self-efficacy had no direct impact on self-disclosure, it interacted with consumer information about negative outcomes of privacy disclosures -- what have variously been called privacy concerns, fears, or risks. Highly self-efficacious consumers were unaffected by information about negative consequences, but those with little self-efficacy were unlikely to supply personally identifying information when they were made aware of the potentially harmful side-effects of such disclosures. This interaction effect may well be obscured in cross-sectional survey studies where consumers with differing levels of privacy self-efficacy are lumped together. And, the studies that seemed to indicate that privacy did not matter may rather provide evidence that many consumers are unaware of their true privacy risks or are (over) relying on third party certifications and other peripheral cues to allay their concerns. In other words, privacy does matter, but not when consumer confusion and misinformation reign."

2008

Title Car Rental Contracts: Business practices, contract terms and consumer protection	
published in Report of the ECC Ireland, 2008. Online publication: http://www.eccireland.ie/	
Year 2008	Authors European Consumer Centre Ireland
Setting of the experiment "The report focuses on the business practices, contract terms and consumer protection in the car rental industry in Ireland. The key objectives of this study are to: - Analyse the complaints related to the car rental sector received by ECC Ireland in 2007. - Determine the trends and central problem areas. - Scrutinise standard car rental contracts in light of the new legislation. - Propose recommendations."	
Research question Assessing the efficacy of standard agreements used in the car rental sector form the consumer's point of view	
Results *(copied from abstract/conclusions of the publication)* "The main observations are that despite an overall decrease in the amount of car rental complaints received by ECC Ireland, the number of disputes against Irish based companies increased. It is apparent from analysis of the complaints that most of the difficult areas are the result of unclear, misleading or unfair contract terms. The provisions in standard contracts are not a violation of the legislation in all cases but there is a lot of space for improvements to make the contracts more transparent and customer friendly." "Policies in [these] area[s] should be reviewed to make sure they are in conformity with the Consumer Protection Act and the legislation on Unfair Terms in Consumer Contracts. [...] The role of the Alternative Dispute Resolution (ADR), voluntary codes of conduct, standard complaint forms and consumer awareness aimed at increasing the standards of service within the industry should not be underestimated. Further developments in these areas should be encouraged. Finally, it should be pointed out that any improvements will require broad agreement between all the parties involved to become truly successful. [...]"	

Title The Cost of Reading Privacy Policies	
published in I/S: A Journal of Law and Policy for the Information Society, http://www.is-journal.org/	
Year 2008	Authors Aleecia M. McDonald and Lorrie Faith Cranor
Setting of the experiment The authors calculated the „time to read privacy policies in two ways. First, we used a list of the 75 most popular websites [from AOL search data in October, 2005] and assumed an average reading rate of 250 words per minute to find an average reading time of 10 minutes per policy. Second, we conducted an online study of 212 participants to measure time to skim online privacy policies and respond to simple comprehension questions." "We asked five questions including "Does this policy allow Acme to put you on an email marketing list?" and "Does the website use cookies?" All answers were multiple choice, rather than short answer, so the act of answering should not have substantially increased the time to address these questions." "We used data from Nielsen/Net Ratings to estimate the number of unique websites the average Internet user visits annually with a lower bound of 119 sites. We estimated the total number of Americans online based on Pew Internet & American Life data and Census data. Finally, we estimated the value of time as 25% of average hourly salary for leisure and twice wages for time at work."	
Research question „We pose the question: if website users were to read the privacy policy for each site they visit just once a year, what would their time be worth?"	
Results *(copied from abstract/conclusions of the publication)* „In this paper we contend that the time to read privacy policies is, in and of itself, a form of payment." "Given that web users also have some value for their privacy on top of the time it takes to read policies, this suggests that under the current self-regulation framework, targeted online advertising may have negative social utility." "The Bureau of Labor Statistics finds an average hourly wage of $17.93 for March, 2008.[52] That gives us estimates of $35.86/hour for the opportunity cost of reading privacy policies at work and $4.48/hour for the opportunity cost of reading privacy policies at home." "We estimate that reading privacy policies carries costs in time of approximately 201 hours a year, worth about $3,534 annually per American Internet user. Nationally, if Americans were to read online privacy policies word-for-word, we estimate the value of time lost as about $781 billion annually."	

Title What Californians Understand about Privacy Online	
published in UC Berkeley. 3 September 2008. Research Report.	
Year 2008	Authors Hoofnagle, C.J.; King, J.
Setting of the experiment The "survey questions were asked as part of the 2007 Golden bear Omnibus Survey, a telephone-based survey of a representative sample of California residents conducted by the Survey Research Center of University of California, Berkeley." "The dual frame sample used random digit dialing of both cell phones and residential landline telephones, with one respondent per household selected. English and Spanish speakers over the age of 18 were eligible. 1,186 respondents completed the telephone interview, conducted form April 30th to September 2nd, 2007 […]. However, in order to include more questions in the survey than could be administered to all respondents in a reasonable period of time, the sample was divided into six randomized parts or units. All respondents were asked certain basic demographic and background questions, but most questions were administered only to 5/6th of the complete sample. This reduced the number of respondents who answered [the] questions to 991."	
Research question Assessment of "Californians' understanding of privacy policies."	
Results The researchers found out that "California consumers believe that privacy policies guarantee strong privacy rights. The term "privacy policy" is functioning in consumers' minds as a privacy seal. A majority of Californians believe that privacy policies guarantee the right to require a website to delete personal information upon request, a general right to sue for damages, a right to be informed of security breaches, a right to assistance if identity theft occurs, and a right to access and correct data. In other cases, a majority believes that privacy policies prohibit common business practices, or simply doesn't know the answer to the question. For instance, a majority either doesn't know or believes that privacy policies prohibit third party information sale, affiliate sharing, government access to personal information, and enhancement. It is privacy policies guarantee strong privacy rights."	

2009

Title Timing Is Everything? The Effects of Timing and Placement of Online Privacy Indicators	
published in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems: 319-328.	
Year 2009	Authors Serge Egelman, Janice Tsai, Lorrie Faith Cranor, Alessandro Acquisti

Setting of the experiment

Egelman et al. “created a controlled privacy premium”, “in order to quantify differences in purchasing behaviors”: “participants who wanted a higher degree of privacy would have to pay a fixed amount for it.” They “also wanted to determine whether participants’ behaviors would differ when purchasing a product that did not raise additional privacy concerns compared to a product that did.”

They “designed the laboratory experiment to test the following hypotheses:

1. Participants will pay for increased privacy when they see privacy indicators.
2. Participants who see privacy indicators will pay more for the privacy-sensitive item than the item that does not raise additional privacy concerns.
3. Participants will be more likely to pay for increased privacy when they see privacy indicators alongside search results before visiting a website than when they see privacy indicators after clicking on search result links.
4. Participants will be more likely to pay for increased privacy when they see privacy indicators before they see the content of a website than when they see privacy indicators alongside the content of a website.
5. Participants who see privacy indicators after clicking on search result links will visit more websites than those who see privacy indicators alongside search results.

They “conducted a laboratory experiment during the summer of 2008 using participants from the Pittsburgh area. We recruited 89 participants using Craigslist and flyers on bus stops, telephone poles, and community bulletin boards.” They “used a screening survey to gather basic demographic data and to assess privacy concerns related to using the Internet and online shopping.” “Based on this requirement, [they] screened out 16.39% (50 of 305) responses.”

The authors “chose a specific vibrating sex toy, the “Pocket Rocket Jr.,” as the privacy-sensitive item” and an “8-pack of Duracell AA batteries as the item unlikely to raise additional privacy concerns beyond the act of providing personal information to an online vendor.”

Research question
Examination of “whether the timing and placement of online privacy indicators impact Internet users’ browsing and purchasing decisions.”
Results
(copied from abstract/conclusions of the publication)
“In this paper we showed that the timing of privacy information display impacts purchasing decisions: participants who decided to visit only one website to make their purchases paid significantly more money for a higher level of privacy when privacy indicators were presented alongside their search results; similar participants who did not see privacy indicators until after they had already selected a website were unwilling to spend time finding websites with higher privacy levels and instead made purchases from cheaper websites. Likewise, participants who did comparison shopping were just as willing to use interstitial and frame privacy indicators to find websites with higher privacy levels, even though this meant visiting significantly more search results. Finally, we observed that privacy decisions depended on privacy concerns surrounding the items being purchased: participants had greater privacy concerns when making the sex toy purchases and therefore went out of their way to use the privacy indicators to find websites that offered higher levels of privacy, even if this meant paying a premium. Likewise, many participants were not willing to pay a privacy premium for the batteries because the product did not trigger the same level of privacy concern as the sex toy.”

Title	
Better Information Handbook	
published in	
Advice Services Alliance. London (funded by the Ministry of Justice UK)	
Year	Authors
2009	Advice now (Webber, M.; Harris, T.; Jones, M.)
Setting of the experiment	
This is a handbook with several tips how to produce better information.	
Research question	
How to produce better information?	
Results	
(copied from abstract/conclusions of the publication)	
“This handbook aims to fill this gap. It discusses the issues involved in the successful delivery of information on law-related issues to the public, draws together existing good practice, and provides practical advice on techniques and procedures. In doing this, it aims to stimulate debate on the best ways to produce this type of information and improve the general quality of what is produced.”	

Title Nudging Privacy. The Behavioral Economics of Personal Information	
published in Security & Privacy Economics IEEE (November/December 2009): 72-75 (pre-publication version)	
Year 2009	Authors Alessandro Acquisti
Setting of the experiment The author applied different "theories and methodologies from behavioral economics and behavioral decision research to investigate privacy decision making."	
Research question „What drives individuals to reveal, and to hide, information about themselves to and from others?"	
Results *(copied from abstract/conclusions of the publication)* „In the course of various studies, colleagues and I have found, for instance, that individuals are less likely to provide personal information to professional-looking sites than unprofessional ones, or when they receive strong assurances that their data will be kept confidential. We've found that individuals assign radically different values to their personal information depending on whether they're focusing on protecting data from exposure or selling away data that would be otherwise protected. We've found that they might also suffer from an illusion of control bias that make them unable to distinguish publication control from control of *access* to personal information."	

Title A Comparative Study of Online Privacy Policies and Formats	
published in Privacy Enhancing Technologies, Lecture Notes in Computer Science Volume 5672, 2009, pp 37-55 (authors pre-press version)	
Year 2009	Authors Aleecia M. McDonald, Robert W. Reeder, Patrick Gage Kelley, Lorrie Faith Cranor
Setting of the experiment „We conducted an online study from August to December 2008 in which we presented a privacy policy to participants and asked them to answer questions about it. We posted	

advertisements on craigslist and used personal networks to recruit participants."

They used a between subjects design and divided each participant into one of 15 privacy policy representations. The questions for each participant remained constant, only the policy differed.

They analyzed six companies (Disney, Microsoft, Nextag, IBM, Walmart and O'Reilly) and 749 participants across 15 conditions. The study questions were divided into three groups: Comprehension, Psychological Acceptability and Demographics.

Hypotheses:
– Participants will have (a) higher accuracy scores, (b) shorter times to answer, and (c) greater psychological acceptability with both of the standardized formats than with their natural language counterparts.
– Participants will have (a) higher accuracy scores, (b) shorter times to answer, and (c) greater psychological acceptability with highly readable natural language than they will on natural language policies with low readability metrics.
The author's next step was to remove outliers and perform an ANOVA analysis for time data and psychological acceptability.

Research question

This paper contains an evaluation of three different formats for privacy policies and a comparison of policies from six different companies.

Results

(copied from abstract/conclusions of the publication)

„We evaluated three formats in this paper: layered policies, which present a short form with standardized components in addition to a full policy; the Privacy Finder privacy report, which standardizes the text descriptions of privacy practices in a brief bulleted format; and conventional non-standardized human-readable policies. We contrasted six companies' policies, deliberately selected to span the range from unusually readable to challenging. Based on the results of our online study of 749 Internet users, we found participants were not able to reliably understand companies' privacy practices with any of the formats. Compared to natural language, participants were faster with standardized formats but at the expense of accuracy for layered policies. Privacy Finder formats supported accuracy more than natural language for harder questions. Improved readability scores did not translate to improved performance. All formats and policies were similarly disliked."

"As compared to natural language, we found that layered policies led to lower accuracy scores for topics not in the short layer. Privacy Finder was indistinguishable from natural language until questions became harder, at which point Privacy Finder was slightly superior to natural language."

"Our hypotheses were not fully supported and in some cases were refuted. Both layered and Privacy Finder formats did improve times to answer, but not by much, and at the expense of accuracy for layered policies. Privacy Finder policies showed modest

improvement in accuracy for complex questions but no improvement for easy questions. While the accuracy scores for Privacy Finder were low in some cases, the format does represent a step forward from the status quo. Readability did not determine outcomes for natural language policies. For natural language, in some cases it appears the practices of the company were greater determinants than the words they used to describe those practices. We found few statistically significant differences in psychological acceptability."

2010

Title	
The Economics of Personal Data and the Economics of Privacy	
published in	
Background Paper No. 3, Joint WPISP-WPIE Roundtable: “The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines”, 1 December 2010	
Year	Authors
2010	Alessandro Acquisti
Setting of the experiment	
This document has been prepared as background to for the Roundtable of the OECD Working Party for Information Security and Privacy (WPISP) and Working Party on the Information Economy (WPIE). “It provides an overview of the economic analysis of the protection and revelation of personal data. In particular, it (1) describes the evolution of the economic theory of privacy, (2) examines privacy-related trade-offs for data subjects and data holders, and (3) highlight the current economic debate on privacy protection.”	
Research question	
Examination of privacy from an economic perspective and highlight how a co-regulatory mix of economic findings, privacy-enhancing technology and regulatory intervention could nudge the market to enhance privacy.	
Results	
(copied from abstract/conclusions of the publication)	
Considering the conflicting analyses the paper presents, “the only straightforward conclusion about the economics of privacy and personal data is that it would be futile to attempt comparing the aggregate values of personal data and privacy protection, in search of a “final,” definitive, and all-encompassing economic assessment of whether we need more, or less, privacy protection. Privacy means too many things, its associated trade-offs are too diverse, and consumers valuations of personal data are too nuanced.	
(...) In this author’s opinion, however, investigating privacy from an economics angle can help to “find a balance between information sharing and information hiding that is in the best interest of data subjects but also of society as a whole. (...)” The author concludes that self-regulatory, market-driven solutions may achieve a balance between information sharing and information hiding, accompanied by user awareness or education programs, consumer-focused privacy enhancing technologies, and user controllable privacy solutions.	
Regulators` interventions aimed at fostering the dissemination and adoption of privacy enhancing technologies, may help to reach a desirable economic equilibrium. “In such a co-regulatory framework, economics could highlight different trade-offs, technology	

could help achieve more desirable equilibria, and regulatory intervention could nudge the market to adopt those technologies." The "burden of proof could be also extended to the data holders, who may be requested to demonstrate why they cannot efficiently keep providing the same products and services in manners that are more protective of individual privacy".

Title The Law of Standard Form Contracts: Misguided Intuitions and Suggestions for Reconstruction	
published in DePaul Business & Commercial Law Journal, Vol. 8: 199-227	
Year 2010	Authors Shmuel I. Becher, Esther Unger-Aviram
Setting of the experiment "The first study in this essay focuses on the intent of consumers to read form contracts in four different scenarios. The second examines the extent to which prevalent rational-economic factors influence potential consumers in their intent to read form contracts." <u>Study 1: Do Consumers Read Their Contracts?</u> "One hundred and forty-seven respondents volunteered to fill out a questionnaire. The population that participated in this study was a heterogeneous group of students from two different academic institutions. […] At least 48 of the respondents were females and at least 89 respondents were males (10 respondents did not indicate gender), with various income levels." "Two versions of the questionnaire were designed to examine the propensity of individuals to read SFCs. Each version included two ex ante and two ex post scenarios, and contained four different types of scenarios that any individual respondent was likely to encounter, some more often than others, some of higher cost and value than others. The different scenarios allowed [the author] to examine how far generalizations about consumer tendency to behave consistently in all ex ante and ex post scenarios could be made. Each version included scenarios that occurred in the following four consumer-business relationships: bank, car-rental agency, laundry services, and prestigious nursery school. The first three scenarios, although different in context, are similar in that they do not concern the wellbeing of a dependent individual (i.e., a child). In these scenarios, any wrongdoing may result in monetary damages, some greater than others. The fourth scenario, the nursery school, differs from the other three in that not only monetary damage may be incurred, the physical and mental wellbeing of a dependent child may be at risk also. Therefore, although this scenario indeed portrays a situation that one may commonly encounter, the responsibility and potential damage and loss are of a different nature and may therefore call for more cautious behavior on the	

consumer's part. Put differently, these diverse scenarios allowed [the authors] to examine whether consumers' behavior might depended on the particular context of the SFC at stake. The questionnaires were randomly distributed to the participants. Each participant filled out one questionnaire."

Study 2: Rational-Economic Factors

The author designed a "second questionnaire, to clarify further the main factors that lead consumers to read (or not to read) SFCs." In other words, in this step the authors examine "whether and to what degree rational-economic factors influence consumers' intent to read a car rental SFC, both ex ante and ex post."

"One hundred and twenty respondents volunteered to fill out questionnaires. All were students studying toward a Master's degree […], or a Bachelor's degree […]. At least 65 respondents were females and at least 47 were males (8 respondents did not indicate gender), with various income levels."

They examined one ex ante scenario and one ex post scenario. "The list of factors appearing after each scenario was: size of the writing (font) used in the contract; density of the print; the (monetary) cost of the car rental; length of the contract (number of pages); type of language used in the contract (legal wording, terms, definitions); opportunity to improve or change the contract terms and conditions through negotiation; opportunity to learn important things about the car rental transaction that were not indicated by the salesperson; and the assumption that the other car rental counters would offer contracts with similar conditions and terms. On both the ex ante and the ex post scenarios, the volunteers were asked to rate each of the factors on a 1–7 Likert-type scale from 1= no influence, through 4= some influence, to 7=very strong influence."

Research question

The "assumptions and propositions that appear in the literature on consumers' reading patterns and contracting behavior largely rely on personal belief or intuition." "This essay explores these intuitions and examines intended consumer behavior in common contracting contexts."

The authors are focusing on two questions: "first, whether consumers read their form contracts; second, what factors influence consumers' contracting behavior."

Results

(copied from abstract/conclusions of the publication)

Study 1 – Ex Ante Atage

The authors "first hypothesis was that most consumers do not read SFCs in their entirety at the ex ante stage. In the car rental scenario a large majority of the respondents, 81% [..], stated that they would not read the contract in its entirety. However, 60% of the respondents […] indicted that they would skim through or read parts of it prior to signing. In the bank account scenario 92% of the respondents […] said that they would not read the contract in its entirety. Again, a substantial proportion of the respondents, 47% […], indicated that they would skim through or read parts of

the contract before signing. As expected, a solid majority indicated no intention to read SFCs in one of ex ante scenarios of the second version as well. In the laundry scenario 75% of the respondents […] reported that they would not read the contract in its entirety. Consistent with the previous two ex ante scenarios, 61% of the respondents […] indicted that they would either skim through or read selected parts of the contract prior to signing. The results in these three scenarios have much in common. In all three cases large majorities indicated no intention to read the SFCs in their entirety. Yet, a large proportion of the respondents stated their inclination to skim though the contract or read it selectively Interestingly, different results were found in the nursery school scenario. Here, only 24% […] indicated no intention to read the contract in its entirety. […] An additional 17% […] said that they would either skim through or read only selected parts of the contract prior to signing it. The remaining 7% […] indicated that they would sign the contract without reading it, but intended to read it at a later time.

Thus, the hypothesis that the vast majority of consumers do not read SFCs receives partial support. In three out of the four scenarios (i.e., bank, laundry, car rental scenarios) consumers indeed reported that they would not read SFCs in their entirety at the ex ante stage. By contrast, in the nursery school scenario most consumers reported an inclination to read the contract in its entirety prior to signing. Therefore, the hypothesis is partially supported."

Their "second hypothesis was that a substantial minority–at least a third– of consumers are inclined to read SFCs in their entirety at the ex ante stage, thus disciplining sellers. […] These analyses show that in two scenarios – the car rental and the bank account – a significantly smaller proportion than one third (33.3%) of the consumers reported a tendency to read the contract ex ante […]. In the laundry scenario 18/72 (25%) of the respondents indicated that they would read the contract ex ante. […] Of course, in the nursery scenario, a proportion significantly larger than one third indicated that they would tend to read the contract ex ante […]. Thus, in two scenarios (car rental and bank) out of the four, the proportion of the consumers that report a tendency to read the entire contract ex ante was significantly smaller than the assumed one third."

Study 1 – Ex Post Stage

The authors "third hypothesis was that the proportion of consumers who read SFCs ex post […] will be significantly larger than the proportion who read them ex ante […]." "Indeed, a significantly larger proportion of consumers were found to report intent to read the contract ex post (rather than ex ante) in three out of the four scenarios: car rental,[…] bank account, […] laundry […] Once again, the only exception was the nursery school scenario, in which a significant majority of the respondents indicated that they would read the entire contract before signing it […]."

Study 1 – Conclusion

"The first study showed that some consumers read some of their contracts some of the time. It also demonstrated and that some contracts are read significantly more often than others."

Study 2 – Ex Ante Stage

The factors that most strongly influenced consumers' intent to read the SFC ex ante were cost of transaction, length of contract and opportunity to change/improve contract terms. The factors that ranked lowest on intent to read ex ante include contract density, font size, and legal language." This "indicates that although all of the factors had an impact on intent to read SFCs ex ante, cost of transaction, length of contract and opportunity to change/improve contract terms had a significantly stronger impact in comparison to the other remaining factors (i.e., similarity to other car rental contracts, density, opportunity to learn new things about the contract, font size, and legal language)."

Study 2 – Ex Post Stage

"The factors that most strongly influenced consumers' intent to read the SFC ex post were cost of transaction, opportunity to learn new things, and opportunity to change/improve contract terms. The factors that ranked lowest on intent to read ex post include length of contract, contract density, and font size. […] This indicates that although all of the factors had an impact on intent to read SFCs ex post, cost of transaction and the opportunity to learn had a significantly stronger impact in comparison to the other remaining factors (i.e., opportunity to change/improve contract terms, legal language, length of contract, density, and font size)."

Study 2 – Conclusion

"In general terms, all the factors examined in this study clearly influence consumers' intended contracting behavior. However, some factors are more dominant than others."

"[…] all these findings should serve policy makers and courts in better designing the law that governs consumer form contracts."

Title	
Trained to Accept? A Field Experiment on Consent Dialogs	
published in CHI '10 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Atlanta, Georgia, USA: pp 2403-2406	
Year 2010	Authors Rainer Böhme, Stefan Köpsell
Setting of the experiment „An opportunity for our field data collection was given between May 20th and July 20th, 2008, when the operators of the free Internet anonymity service AN.ON/JonDonym (http://anon.inf.tu-dresden.de) initiated a study to measure the security of their service against a new kind of threat. Their research required an update of the client software and the operators found it appropriate to let the users decide whether they would like to	

participate in the measurement process or not. The operators agreed to implement this consent dialog with 2x2x3 experimental conditions designed by us, and assigned them to users randomly and independently. User reactions were measured by the participation rate (i. e., fraction of users who approved the request), whether or not further information was consulted in the online help, and by the time elapsed to make a decision (response latency). The client software update was enforced for all users, each at a random time (for server-side load balancing). The intended user experience was an interruption of anonymous web access. This mimics the distraction from primary tasks that is characteristic for interception dialogs. Our sample of users of an anonymity tool is certainly not representative. It is biased towards above-average computer literacy and concerns about online privacy: AN.ON users make efforts to install the client software, reconfigure their web browsers, accept a small bandwidth, and differ in attitudes and motivations with regard to online privacy. The bias is not a serious problem, as our results can be interpreted as best-case bounds. If even highly concerned individuals are unresponsive to relevant decisions about their security, then the average user cares even less. By contrast, other research has been criticized of diluting results by including too many indifferent subjects. Sunshine et al. complemented their study with a sample of security experts." The main data set contains 81,920 user responses.
Research question Do requests and button texts pointing to a voluntary decision decrease the probability of consent?
Results *(copied from abstract/conclusions of the publication)* "A typical consent dialog was shown in 2_2_3 experimental variations to 80,000 users of an online privacy tool. We find that polite requests and button texts pointing to a voluntary decision decrease the probability of consent — in contrast to findings in social psychology. Our data suggests that subtle positive effects of polite requests indeed exist, but stronger negative effects of heuristic processing dominate the aggregated results. Participants seem to be habituated to coercive interception dialogs — presumably due to ubiquitous EULAs — and blindly accept terms the more their presentation resembles a EULA. Response latency and consultation of online help were taken as indicators to distinguish more systematic from heuristic responses."

Title Misplaced Confidences: Privacy and the Control Paradox
published in Ninth Annual Workshop on the Economics of Information Security (WEIS). June 7-8 2010

Year	Authors
2010	Brandimarte, L.; Acquisti, A.; Loewenstein, G.

Setting of the experiment

In order to test their hypotheses the authors designed three randomized experiments. "All three experiments were survey-based and subjects were recruited among students at a North-American University. The design of the first two experiments was essentially the same […]."

Experiment 1:

"Experiments 1 and 2 manipulated subjects' sense of control in order to make them feel less in control over information publication, relative to a baseline condition of direct control."

"For the first two experiments, the questions contained in the survey were the same […]. The surveys focused on students' life in the city around the university and on campus […]. The justification for the survey was the creation of a new university networking website that would be launched at the end of the ongoing semester. Students were invited to become members of the network. […] The questions varied in terms of level of perceived privacy intrusiveness."

"In one condition (Condition 1) subjects were told that a profile would be automatically created for them, containing the information they provided, and that this profile would be published online once the website was completed, without any intervention by the researcher. In the other condition (Condition 2) subjects were told that a researcher would have collected the data, created a profile for them and published it on the network. The manipulation focused on how much control subjects had on the publication of their information. In Condition 1, subjects were given more control over the publication of their information: they decided exactly what to publish, if they wanted to publish anything at all. In Condition 2, on the other hand, an unknown "researcher" was responsible for the publication of their information: if subjects decided to disclose, they may have been somewhat less sure about what would happen to their information, because it ended up in possession of a researcher."

Collectively, the "survey contained 40 questions: seven highly intrusive questions, seven moderately intrusive questions and 24 non-intrusive questions […]."

The "dependent variable was whether a subject answered to a certain question: to test hypothesis H1, [the authors] considered whether the subject decided to answer or not a question; to test hypothesis H2, [the authors] considered whether the subject decided to answer the more privacy intrusive questions. If, indeed, [the] subjects are affected by the paradox of control, they would be willing to answer more questions - and, specifically, more sensitive questions - in Condition 1 (where they felt personally responsible for the publication of that information) than in Condition 2 (where a researcher stood between them and the online publication)."

Experiment 2:

"Study 2 mimicked Study 1's design" but the authors "changed the control manipulation. Condition 1 remained unaltered with respect to Study 1, while in Condition 2 participants were told that a 50% subset of the profiles created would have been randomly picked and published on the new university networking website."

They also constructed a new "hypothesis which will then be alternative to H1:

> H1b: If people care less about the study overall, they will be willing to reveal more if they have control over information publication, and particularly so for time-consuming questions."

Experiment 3:

"Experiment 3 […] manipulated subjects' sense of control in order to make them feel more in control over information publication, relative to a baseline condition."

"The alleged motivation for the survey was that we were interested in studying "ethical behaviors" and that we would ask a series of questions related to this topic. The survey consisted of ten yes/no questions regarding more or less sensitive and moot behaviors, such as stealing, lying or consuming drugs […]. Subjects were informed that none of the questions required an answer. Subjects were also told that the researchers were meaning to publish the answers provided by the participants in a Research Bulletin among the results of the study, but no detail was given as to whether this Bulletin would have been printed or published online, nor as to whom this Bulletin would have been visible/available to. What is relevant is that, similarly to the first two studies, subjects had no control over the access to, or the usage of, their information by others. Besides the ten questions on ethical behaviors, subjects were asked to provide some demographic information […] and some final questions needed as manipulation checks. Subjects were randomly assigned to one of five conditions. What varied was the control subjects had over the publication of the answers they would provide."

Research question

Testing of the "hypothesis that mere control over publication of private information affects individuals' privacy concerns and their propensity to disclose sensitive information even when the objective risks associated with such disclosures do not change or […] worsen."

Hypothesis:

> H1: "If people suffer from the paradox of control over private information, they will be willing to reveal more [less] if they have more [less] control over information publication, even if their control over access and use of that information by others remains unaltered."
> H2: "If people suffer from the paradox of control over private information, they will be willing to reveal more sensitive information if they have control over information publication, even if their control over access and use of that information by others remains unaltered."

Paradox of control over private information: “individuals reveal more when they feel in control over information dissemination, regardless of the actual level of control over access and usage.”
Results The authors “found that people respond to manipulations of control over information publication, while the control over information access and use by others remained unchanged.” They “can thus infer that control over publication receives a larger weight in people’s decision to reveal. Even though people are likely to be aware that potential privacy threats derive from who accesses their information and how that information is used, they may neglect to fully consider, or even fail to realize, that control over information access and usage by others is what matters most for privacy protection, while control over information publication is less relevant: [their] subjects seemed to care more for control over publication of private information than for control over access and use of that information; when someone other than themselves was responsible for the publication, or when the publication itself was uncertain (which reduced the probability of access/use by others) [their] subjects were more likely to refrain from disclosing. This could be due to the fact that, since the publication of personal information is a certain and immediate event, it is also more salient than the risk of somebody accessing and using that information, an outcome which is uncertain and distant in time. […] Arguably, the costs and benefits associated with the mere dissemination of personal information are psychological, while the trade-offs arising from other people’s actual usage of our information are more tangible: social value, promotions, discrimination, and so forth. However, it would appear that individuals give more relevance to the former rather than to the latter trade-offs.”

Title Beliefs and Behaviors: Internet Users’ Understanding of Behavioral Advertising	
published in 38th Research Conference on Communication, Information and Internet Policy, Telecommunications Policy Research Conference. 2 October 2010	
Year 2010	Authors McDonald, A. M.; Cranor, L. F.
Setting of the experiment McDonald et al. followed a two-part approach. First they “performed a laboratory study to identify a range of views through qualitative interviews.” After that they ”conducted an online survey to test and validate our qualitative results.” In the first study, McDonald et al. “performed a series of in-depth qualitative interviews with 14 subjects who answered advertisements to participate in a university study about Internet advertising. Subjects were not primed for privacy. [The authors] followed a	

modified mental models protocol of semi-structured interviews, using standard preliminary questions for all participants, then following up to explore participants' understanding. [The] study ran from September 28th through October 1, 2009 in Pittsburgh, PA. [The authors] recruited participants with a notice on a website that lists research opportunities. Participants were compensated $10 for an hour of their time." In the second study, the authors "recruited 314 participants from the Mechancal Turk web site at the end of April, 2010. The authors "deliberately started the study with short-answer questions to encourage people not to take the survey unless they were willing to invest some time, and used the reasonableness of responses to short-answer questions to screen participants."
Research question "This paper presents empirical data on American adult Internet users' knowledge about and perceptions of Internet advertising techniques."
Results McDonald et al. found "a gap between the knowledge users currently have and the knowledge they would need to possess in order to make effective decisions about their online privacy." "Most users understand that cookies store data on their computers, enable tailored ads, and allow tracking across sites. They are unclear on important details like whether cookies may be combined with other data, what data is stored in cookies, if blocking cookies preserves geolocational privacy, and they are particularly unclear about laws and law enforcement. Web browsers may contribute to users' confusion." Furthermore, the authors found that people are "generally unwilling to pay for privacy, not because they do not value it, but because they believe it is wrong to pay. Paying to keep data private was termed 'extortion' by some participants." They "also found a gap between willingness to pay to protect data and willingness to accept a discount in exchange for releasing the same data. People may ascribe more value to what they possess. People may value their privacy less when presented with an opt-out for data collection, which suggests data belongs to the company collecting it, rather than an opt-in choice for data collection, which suggests data belongs to the individual."

2011

Title Information gut, alles gut? [Information good – everything good?]	
published in Verbraucherzentrale Bundesverband [Federal Consumer Authority]	
Year 2011	Authors Verbraucherzentrale Bundesverband
Setting of the experiment Publication describes requirements for good information practices	
Research question What are quality indicators for good information?	
Results *(copied from abstract/conclusions of the publication)* Criteria described in detail include: - correctness - relevance - access to information - adequacy - attractiveness of presentation - transparency - user-oriented information	

Title Transforming consumer information	
published in Transforming consumer information. A study conducted by the Consumer Information Working Party, 26 October 2011, Working paper	
Year 2011	Authors Alan Richie, Joshua Corrigan, Sandra Graham, Andrew Hague, Alan Higham, Jenny Holt, Philip Mowbray

Setting of the experiment Study based on literature review
Research question Analysing “the current state of consumer information for long-term savings and investments in the UK” and proposing a model for the future.
Results *(copied from abstract/conclusions of the publication)* The authors found strong “evidence that lifestage and personal life events [have an] impact on the financial decisions that households make to accumulate wealth. This suggests that more targeted approaches to consumer segmentation by financial services providers would be beneficial when preparing consumer information rather than adopting a one-size-fits all mentality. A single approach, which fails to acknowledge the potential lifestage of each consumer, may act as a barrier to engagement and understanding. Generic communications which are aimed at all consumers could be failing to convince the majority that there are appropriate investments to meet their specific objectives.” Furthermore, “there are a number of patterns between consumers using the financial services market and how they prefer to seek out information about financial products. […] Judicious targeting of consumer information will be most effective if it both acknowledges the lifestage triggers and is delivered through the most comfortable medium for consumers.” “Most information supporting long term savings and investments is product driven with particular focus around the point of sale. There is little, if any, personalisation to the needs and goals of individual consumers. There are inconsistencies in the type and detail of information provided […]. So whilst communications may meet the FSA’s Treating Customers Fairly outcomes on a stand-alone basis, there is a danger the lack of consistency across products and providers is a barrier to meeting outcome 3 overall. These issues need to be addressed to better engage with consumers.” The authors also claim that “greater application of Behavioural Economics can help […] deliver more effective consumer information. This can be as simple as reducing the number of options available to make action easier or, where appropriate, the use of default options for consumers.” “There are a number of examples where inadequate consumer information has contributed to significant financial loss – both for customers […] and the industry. Typically this has been because a) the key risks of an investment were not adequately explained or linked to the chances of achieving the consumer’s original goal; and b) there was a lack of effective ongoing communication once the product was sold.”

Summarized:

- “The need for a segmented and tiered approach to consumer information. A one-size-fits-all method does not work with known consumer behavioural traits.
- The need to make the most relevant risks central in the information provided. This requires understanding of the consumer’s objectives for their investment.
- The need for an ongoing relationship with consumers (whether adviser, provider or employer), rather than the current bias towards point-of-sale.
- The importance of a consistent consumer journey throughout the duration of their investment.
- The importance of learning from Behavioural Economics when designing communications, rather than only focusing on Plain English rules.”

In the last section the authors “define a possible framework for the provision of information to consumers of long-term savings and investment products that aims to address the issues described [above].” Their framework based upon 3 principals: (1) “Information should relate to a consumer’s financial goals”, (2) “the delivery of Consumer Information should facilitate consumer engagement”, and (3) “consumer Information should be free of bias”.

For implementing such a model the authors recommend 5 steps:

- “Championing cultural change with providers of information
- Grasping the opportunity of regulatory reviews
- Applying a consistent approach to financial projections for consumers
- Providing independent decision aids for consumers
- Introducing an independent watermark of quality
- Exploring how best to communicate financial risk”

Title	
Charter of the Task Force on Smart Disclosure: Information and Efficiency in Consumer Markets	
published in Released from the Committee on Technology, National Science and Technology Council	
Year 2011	Authors National Science and Technology Council
Setting of the experiment guideline and position paper	

Research question
Introduction and depiction of the Task Force on Smart Disclosure (TFSD), which was established in 2012.
Results *(copied from abstract/conclusions of the publication)* "The TFSD will develop guidelines based on best practices for making data from consumer markets available and useful for consumer decision-making." They "determine that the reestablishment of the Task Force on Smart Disclosure: Information and Efficiency in Consumer Markets is in the public interest in connection with the performance of duties imposed on the Executive Branch by law, and that such duties can best be performed through the advice and counsel of such a group." There are several departments and agencies represented on the TFSD. The TFSD can also seek advice from the private sector.

Title	
The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study	
published in Information Systems Research, Vol. 22, No. 2, June 2011, pp. 254–268	
Year 2011	Authors Janice Y. Tsai, Serge Egelman, Lorrie Faith Cranor, Alessandro Acquisti
Setting of the experiment The study consists of three parts: "(1) an online concerns survey to determine what types of privacy concerns and products to include in the experimental part of the study; (2) an online shopping experiment to investigate how the prominent display of privacy information affects the purchase behavior of privacy-minded users; and (3) a post experiment interview." "Participants had to be at least 18 years old, have a personal credit card to use during the study, and have experience shopping online." Overall they received 272 complete responses. "Hypothesis 1. Participants in the privacy information condition will be more likely than those in the no privacy indicator condition to purchase from websites annotated with icons. Hypothesis 2. Participants in the privacy information condition will be more likely than those in the no privacy indicator condition to purchase from websites annotated with the four-gray-boxes icon (the sites offering the best privacy policy).	

Hypothesis 3A. Participants presented with prominent privacy information (those in the privacy information condition) will be more likely than those in the no privacy indicator condition to pay a premium to purchase from sites that have better privacy policies. Hypothesis 3B. In the absence of prominent privacy information, people will purchase where price is lowest. Hypothesis 4. Icons in the privacy information condition will affect purchase decisions more than icons in the irrelevant information condition.”
Research question „This paper reports on research undertaken to determine whether a more prominent display of privacy information will cause consumers to incorporate privacy considerations into their online purchasing decisions.”
Results *(copied from abstract/conclusions of the publication)* “We designed an experiment in which a shopping search engine interface clearly and compactly displays privacy policy information. When such information is made available, consumers tend to purchase from online retailers who better protect their privacy. In fact, our study indicates that when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites. This result suggests that businesses may be able to leverage privacy protection as a selling point.” “We found that participants in the privacy information condition were more likely to make purchases from websites offering medium or high levels of privacy (even when those sites charged higher prices), and those in the control conditions generally made purchases from the lowest priced vendor. This indicates that individuals are likely to pay a premium for privacy when privacy information is made more accessible. Furthermore, individuals presented with the same indicators as those used for the privacy group — but ostensibly attached to irrelevant merchant features — were less likely to take those indicators into consideration when making purchases. This demonstrates that the observed behavior cannot simply be attributed to an interest in purchasing from websites labeled with attractive indicators.” All hypotheses are supported.

Title	
Nudging Users Towards Privacy on Mobile Devices	
published in	
Proc. CHI 2011 Workshop on Persuasion, Nudge, Influence and Coercion	
Year	Authors
2011	Rebecca Balebako, Pedro G. Leon, Hazim Almuhimedi,

	Patrick Gage Kelley, Jonathan Mugan, Alessandro Acquisti, Lorrie Faith Cranor and Norman Sadeh
Setting of the experiment There has been no experiment but the authors describe their "ongoing work on embedding soft paternalistic mechanisms in location sharing technologies and Twitter privacy agents."	
Research question How can "soft paternalistic solutions (also known as nudges) may be used to counter cognitive biases and ameliorate privacy-sensitive behavior?	
Results "As part of our ongoing research, we are interested in better understanding how different elements of Locaccino functionality effectively nudge people in different directions. [...]. The authors are "experimenting with new interface designs as well as new ways of leveraging some of the machine learning techniques" [...] The Twitter privacy agent is an application we are building to help Twitter users behave in a more privacy protective way. We plan to build tools that will provide nudges that guide users to restrict their tweets to smaller groups of followers or discourage them from sending tweets from mobile devices that they may later regret. We plan to empirically test the impact of these nudges on user behavior. We will also examine whether fine-grained privacy controls result in more or less data sharing. We expect our work on nudges in behavioral advertising, social networks, and location sharing to be effective for improving privacy decisions on mobile devices. We further hope our soft-paternalistic approach to have a broader impact, guiding the development of tools and methods that assist users in privacy and security decision making."	

Title The Role of Affect and Cognition on Online Consumers' Decision to Disclose Personal Information to Unfamiliar Online Vendors	
published in Decision Support Systems 2011(51): 434-445.	
Year 2011	Authors Li, H.; Sarathy, R.; Xu, H.
Setting of the experiment "An experimental Web site was created to allow easy manipulation of sensitivity of information. […] to ensure realism, the interface of the experimental Web site closely mimic a real commercial Web site providing Internet fax service, MyFax […]. Moreover, […] each subject assumed the role of an online shopper seeking internet fax service for	

the purpose of sending resumes for job applications. The subjects were introduced to some of the advantages of Internet fax service over email for job application before interacting with the experimental Web site. […] The experimental web site has a 30-day free trial membership sign-up form, which was used to manipulate information sensitivity. The sensitivity of information was manipulated at two levels: low and high. A common set of information of low to moderate sensitivity that included name, gender, email, and postal address was requested for both low and high sensitivity treatment conditions. Besides the common information, the high sensitivity condition also had requests for telephone number and credit card information." Because this study also measured "whether subject read the privacy policy", privacy policy "was not manipulated in the design." However, subjects were free "to decide whether to read the privacy policy or not. The privacy policy used in the experimental Web site was designed along the lines of a strong privacy policy, i.e. containing all basic elements of FIP principles." "Subjects were randomly assigned to only one of the two treatment conditions, i.e. either low sensitivity or high sensitivity information request. A major task page was used to introduce the task scenario to subjects and provide detailed step by step instructions. Subjects were required to interact with the experimental site as naturally as possible for about 10 min to get an overall impression of the Web site. Then, they were instructed to fill out section I of the survey that measured their initial emotions before information exchange. The next stage of the experiment simulated an information exchange context. Subjects were instructed to evaluate a sign-up form of the company's 30-day free trial program and made aware that they were not required to fill the form with their private information. A link to the vendor's privacy policy was provided at the bottom of the form. They could choose to read the privacy policy if they felt it was necessary. After evaluating the sign-up form, subjects were required to fill out the succeeding two sections of the survey." "Five variables that might influence privacy decisions/behaviors were included in this study as control variables for predicting intention to disclose personal information. They are gender, age, Internet experience, previous experience of being victims of privacy invasion, and media exposure of privacy invasion incidents."
Research question Exploration of "situational factors that influence an individual's online privacy decision-making" using the "privacy calculus framework and the stimulus-organism-response (S-O-R) model to identify both affect-based and cognition-based factors in order to determine the circumstances under which people modify their willingness to provide personal information online." Specifically, they "theorize how initial emotions formed from an overall Web site impression influence privacy-related beliefs (affective lens) and how exchange fairness influences privacy-related beliefs (cognitive lens)."

Results

Data Analysis

They “hypothesized that emotions have a congruent effect on privacy beliefs. This congruent effect was supported. Joy is found to have a significant positive effect on privacy protection belief […] and significant negative effect on privacy risk belief […]. Fear has a significant positive effect on privacy risk belief […]. The relationship between fear and privacy protection belief was not statistically significant.”

Furthermore, “relevance was found to have a significant positive impact on privacy protection belief […] and negative impact on privacy risk belief […]. Sensitivity of information has no significant impact on privacy risk belief […]. Awareness of the privacy policy demonstrating FIP principles was found to significantly enhance privacy protection belief […] but was not significant in shaping privacy risk belief. […] general privacy concern had a significant influence on privacy risk belief […] but was not significant for the formation of privacy protection belief. In all, the model can explain 25.3% of the variance in privacy protection belief and 25.9% of the variance in privacy risk belief. The two privacy beliefs (protection belief and risk belief) and general privacy concern were further found to have a significant impact on behavioral intention to disclose personal information. No control variables were found to be significant. Overall the model could account for 33.7% variance of behavioral intention. The result also suggests that general privacy concern has a significant direct impact on behavioral intention as well as a significant indirect effect on behavioral intention through privacy risk belief.”

Results

“The results of the experiment indicate that, for an unfamiliar Web site, privacy behaviors are driven by both general privacy concern and privacy-related cost–benefit beliefs. Privacy beliefs, in turn, are shaped by general privacy concern, initial emotions and fairness levers. Initial emotions formed from an overall impression of the Web site continue to play an important role in shaping privacy beliefs and decisions, even if subjects are exposed to cognitive processing of information exchange at a later time. Thus, initial emotions have a lasting coloring effect on later stage cognitive processing. Specifically, joy significantly enhances privacy protection belief and reduces privacy risk belief. Interestingly, fear was found to significantly influence privacy risk belief, but not impact privacy protection belief. This finding corroborates the broaden-and-build theory that posits that negative emotions narrow one's momentary thought–action repertoire. […] When online consumers enter the information exchange stage, fairness levers (relevance of information requested and privacy policies) were found to adjust privacy beliefs. As expected, perceived relevance of information requested was found to significantly increase privacy protection belief and reduce privacy risk belief. […] The sensitivity of information was not found to be a significant fairness lever influencing privacy risk belief either directly or through the interaction with perceived relevance. […] Besides perceived relevance, awareness of the privacy policy incorporating FIP principles was found to be another significant fairness lever that enhances privacy

protection belief. […] Surprisingly, awareness of the privacy policy does not significantly reduce privacy risk belief. This may be largely due to the self-commitment nature of a privacy policy, which outlines the level of privacy protection that a Web merchant promises to its consumers. For an unfamiliar Web site, such self-reported guarantee or a privacy policy may not effectively reassure online consumers about the potential risks or unknown consequences of releasing personal information. Finally, general privacy concern was found to significantly increase privacy risk belief and reduce online consumers' information disclosure intention. However, it has no significant impact on privacy protection belief."

The results also "suggest that emotions and fairness levers have about the same contribution in shaping the privacy beliefs and their effects dominate that of general privacy concern." Furthermore, they found that "when an online shopper is interacting with a Web site, his or her privacy beliefs are mainly influenced by situational emotions and fairness levers and his or her privacy beliefs that are formed (situation-specific) play a dominant role in driving his or her intention to disclose personal information. In this process, the effect of general privacy concern is far less important than these situational factors, i.e. emotions, fairness levers and privacy beliefs."

2012

Title Social Media and the Rise in Consumer Bargaining Power	
published in University of Pennsylvania, Journal of Business Law (Vol. 14:3 2012)	
Year 2012	Authors Wayne R. Barnes
Setting of the experiment The article discusses “the law generally applicable to standard form contracts and bargaining, as well as the cognitive and psychological defects that are involved in consumers’ bargaining processes.” Second, it “will discuss several instances where consumers have used social media to obtain favorable resolutions of disputes that were not otherwise required by the terms of the standard form contracts to which they originally agreed when they purchased the goods or services.”	
Research question Does social media has implications for consumer bargaining?	
Results *(copied from abstract/conclusions of the publication)* Standard form contracts are here to stay. They are efficient, and merchants will not sell products or services unless they are able to contractually inoculate themselves against certain types of risks by the inclusion of protective boilerplate (e.g., warranty limitations and exclusions, liability limitations, arbitration clauses, choice of law, etc.). Consumers realize that the contract terms, like most other aspects of a deal, are adhesive in nature—“take-it-or-leave-it.” They don’t have any bargaining power in the formation of the contract. And, even if they did, consumers suffer from multiple cognitive and decision-making defects that would nonetheless preclude their ability to read, comprehend, and negotiate different terms. All in all, consumers have very little bargaining power when they initially decide to transact with a merchant by buying its goods or services. [...] However, because of the unequal power between the parties, the merchant’s frequent decisions to refuse any [...] relief has no immediate consequences, other than loss of the consumer’s repeat business and the limited effects of traditional word-of-mouth discussion of the consumer’s experiences. Simply put, the ironclad nature of the merchant’s protective form contract language, coupled with the enormous bargaining power advantage, results in the merchant being able to effectively deny any relief to the consumer in the face of his disappointed expectations. However, in the world of social media, the landscape is changing. [...] First, at the point of dealing with the disappointed expectations, the merchant and	

consumer are dealing on a much more level playing field information-wise, because the contingency which is the basis of the new dealings between the parties is now a concrete, real event which has in fact occurred, rather than a vague, inchoate possibility of some negative event which conceivably might occur at some point in the distant future. In short, the parties are not dealing in unknown hypotheticals anymore — the thing has happened (e.g., the goods have broken down, or the service has been unsatisfactory), and so both parties know the score. They are not dealing in informational asymmetries that greatly favor the merchant.

Second, and the more obvious point, the consumer is able to wield potentially much more power over the merchant by his or her use of a social media tool to voice his contractual disappointment. If the video, blog entry, tweet, or Facebook post goes "viral," it will rapidly generate exponentially more attention than the consumer's traditional efforts to contact the merchant directly. This can result in enormous pressure on the merchant to rectify the wrong in the court of public opinion. Furthermore, the consumer has achieved this result without necessarily paying any attorneys' fees, litigation costs, or encountering other traditional barriers to achieving a satisfactory remedy against undesirable merchant behavior.

The result is greater empowerment to consumers, or at least the specter of it, in the world of social media and Web 2.0. [...] But its development in the area of consumer contract remedies is a welcomed one. Justice Louis Brandeis famously said, "Sunlight is the best disinfectant." Less famously, but right before that sentence, Brandeis said: "Publicity is justly commended as a remedy for social and industrial diseases." With the advent of the Internet and social media, consumers have the ability to remedy the "disease" of grossly disproportionate bargaining power between behemoth corporate merchants and individual consumers who buy their goods and services. Never before has there been greater ability for consumers to generate publicity, and thus "sunlight," on poor treatment of them by merchants. The result is potentially greater power for consumers, and this is for the good."

Title Automatic Categorization of Privacy Policies: A Pilot Study	
published in School of Computer Science Carnegie Mellon University Pittsburgh, PA 15213	
Year 2012	Authors Waleed Ammar, Shomir Wilson, Norman Sadeh, Noah A. Smith
Setting of the experiment „We used crowdsourced annotations for privacy policy and terms of service documents of 57 websites from the "Terms of Service; Didn't Read" project (http://tos-dr.info). For each website, annotators identified a number of noteworthy terms of these documents	

governing use of the site's services, and gave brief textual descriptions for them such as:

- Deleted images are not really deleted
- Using your real name is optional
- Notifications [of a change in policy] 30 days before changes [take effect]

The set of descriptions is essentially open; in fact half of the descriptions are only used once (i.e., to annotate a single document). A few concepts are repeated (often with rephrased descriptions) multiple times across documents, and some capture concepts related to privacy. The most common concepts in the data are:

- Ability to leave the service (found in 21 policies)
- Transparency on law enforcement requests (found in 19 policies)
- Providing a notice before changing the terms (found in 10 policies)

In addition to the annotated privacy policies, we also collected 794 privacy policies for which we did not have any annotations. Before feature extraction, we preprocessed the privacy policy documents by lowercasing the text and removing punctuation and stopwords."

"We use logistic regression, a classic high-performance probabilistic model, to map privacy policy documents to categorical labels. In this pilot study, there are two labels, corresponding to presence and absence of a concept."

Research question

„We describe a pilot experiment to use automatic text categorization to answer simple categorical questions about privacy policies, as a first step toward developing automated or semi-automated methods to retrieve salient features from these policies."

Results

(copied from abstract/conclusions of the publication)

"Our results tentatively demonstrate the feasibility of this approach for answering selected questions about privacy policies, suggesting that further work toward user-oriented analysis of these policies could be fruitful."

Title	
Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising	
published in	
Proceedings of the Eighth Symposium on Usable Privacy and Security ACM.	
Year	Authors
2012	Ur, B.; Leon, P.G.; Cranor, L. F.; Shay, R.; Wan, Y.

Setting of the experiment

In August 2011, the authors “recruited 48 participants for a combination interview and usability study of privacy-enhancing tools. [...] The study lasted approximately 90 minutes.”

In this paper, they “report on the results of a semi-structured interview that took place in the first 30 minutes of each session. The second part of the study was a usability test, on which [they] have reported separately.”

Part 1: They “began with general questions to explore participants’ attitudes about Internet advertising. Then, [they] asked questions about tailored advertising and interviewees’ knowledge of online tracking mechanisms. To evaluate participants’ knowledge and perception of Internet icons, [they] showed two disclosure icons […].” “The icons and accompanying taglines were first shown alone, and then “in context” on an advertisement. […] [They] spent between five and ten minutes on this first portion of the study.”

Informational video: “The video lasted approximately 7 minutes.”

Part 2: At first, they “evaluated participants’ understanding of behavioral advertising. Then, [they] asked questions about the benefits they perceived for users and other stakeholders. [They] also asked about any negative aspects they perceived in OBA [Online Behavioral Advertising] activities. Next, [they] presented six hypothetical browsing scenarios, asking whether participants would be willing to have information collected about their browsing for the purpose of OBA in each situation. [They] further asked participants about their familiarity with advertising companies and willingness to allow these companies to collect information about their web browsing to tailor ads. Finally, [they] asked participants how they believed they could stop receiving targeted ads if they wanted to do so.”

Research question

Investigation of „non-technical users’ attitudes about and understanding of OBA”

Results

“Participants found behavioral advertising both useful and privacy invasive. The majority of participants were either fully or partially opposed to OBA, finding the idea smart but creepy. However, this attitude seemed to be influenced in part by beliefs that more data is collected than actually is. Participants understood neither the roles of different companies involved in OBA, nor the technologies used to profile users, contributing to their misunderstandings. Given effective notice about the practice of tailoring ads based on users’ browsing activities, participants wouldn’t need to understand the underlying technologies and business models. However, current notice and choice mechanisms are ineffective. Furthermore, current mechanisms focus on opting out of targeting by particular companies, yet participants displayed faulty reasoning in evaluating companies. In contrast, participants displayed complex preferences about the situations in which their browsing data could be collected, yet they currently cannot exercise these preferences. Participants were unaware of existing ways to control OBA. To exercise

consumer choice, participants expected that they could turn to familiar tools, such as their web browser or deleting their cookies. However, mechanisms to exercise choice about OBA in browsers are limited and difficult to use. Deleting cookies, participants' most common response in this study, would nullify consumers' opt-outs. A Do Not Track header has been designed to allow users to set a preference in their browser that does not disappear when cookies are deleted. A handful of companies […] have announced plans to implement this header, although efforts to define fully the meaning of Do Not Track are ongoing in the W3C Tracking Protection Working Group."

2013

Title Nudging People Away From Privacy-Invasive Mobile Apps Through Visual Framing	
published in Human-Computer Interaction–INTERACT. Springer. http://research.microsoft.com/pubs/204872/Interact2013-VisualFraming-CR.pdf	
Year 2013	Authors Eun Kyoung Choe, Jaeyeon Jung, Bongshin Lee, Kristie Fisher

Setting of the experiment

Choe et al. conducted two experiments. For each of them they " created an online experimental setup and recruited participants using Amazon Mechanical Turk (MTurk)." They "made sure no one could participate more than once […]. The studies were available only to U.S. and Canada residents with at least a 95% approval rate […]." They "compensated MTurk participants $0.50 USD per survey for Study 1, and $1 USD per survey for Study 2."

Study 1: Creating Complementary Visuals

"As a first step toward identifying visuals that have higher nudging power, [the authors] investigated whether it is viable to create complementary visual framings that convey semantically equivalent privacy rating information." They "designed two sets of icons: positively-framed (PF) icons using a green plus sign (+) and negatively-framed (NF) icons using a red minus sign (-) […]." They "conducted a between-subjects experiment with two groups: PF icon group and NF icon group."

Participants were asked "to answer two sets of eight icon comparison questions as accurately and quickly as possible." The author showed them "two different privacy ratings and asked which of the two privacy ratings is more privacy-invasive or privacy-preserving […]."

"The dependent measures were accuracy (i.e., the number of correct responses) and task completion time (i.e., average response time per question)."

For the first study the authors "recruited 129 participants and randomly assigned them to either the PF condition (N = 67) or NF condition (N = 62)."

Study 2: Positive vs. Negative Framings

They "tested which visual framing—positive or negative—was more effective in nudging people away from privacy-invasive apps using the icons […] designed in Study 1." They "also explored how people's perception of an app changes if a privacy rating of the app accompanies a user's overall rating (user rating). This resulted in a 2 (framing: PF icon; NF icon) x 3 (privacy rating: high; medium; low) x 2 (user rating: with a user rating of 3; without a user rating) mixed design with repeated measures; framing and user rating

were between-subjects factors and privacy rating was a within-subjects factor, thereby forming four conditions: PF with & without a user rating of 3, and NF with & without a user rating of 3." They "created online surveys for the four conditions. The surveys consisted of three sections: (1) evaluating four apps (one dummy app followed by three apps of varying degrees of privacy ratings), (2) eight Privacy Critics' Rating icon comparison questions, and (3) demographic questions." After showing each app, the authors "measured people's perception toward each app by asking the following four questions: (1) trustworthiness of the app (TRUST), (2) likeability of the app (LIKE), (3) willingness to install the app (INST), and (4) willingness to recommend the app to a friend (RCMD). […] TRUST and LIKE were measured on a 7-point Likert scale, where 1 = not at all trustworthy / I strongly dislike this app, and 7 = very trustworthy / I strongly like this app. INST and RCMD were measured using Yes/No dichotomous questions." For the second study they recruited 235 "participants from Amazon Mechanical Turk and randomly assigned them to one of the four conditions: PF & w/o UR (N = 75); PF & w/ UR (N = 95); NF & w/o UR (N = 79); and NF & w/ UR (N = 83). […] 55% of the participants (N = 129) were male, and 89% of the participants (N = 210) claimed that they own a smartphone."
Research question Investigation of "the effects of […] visual privacy rating, framing, and user rating on people's perception of an app […] through two experiments." RQ1. Can we create complementary visual framings that convey semantically equivalent privacy rating information? RQ2. Do complementary privacy ratings have similar influence on how people perceive an app? If not, is a negative visual framing more effective in nudging people away from privacy-invasive apps? RQ3. Do people's perceptions of an app change if a privacy rating is accompanied by a user rating?
Results *(copied from abstract/conclusions of the publication)* <u>Study 1:</u> "After reading the description and solving eight icon comparison questions, the majority of participants in both groups were able to comprehend privacy ratings in a similar manner. The PF and NF icons resulted in the comparable level of comprehension and speed by survey participants." "The independent samples t-test showed that in terms of accuracy, there was not enough evidence to suggest that PF icon group […] differs from NF icon group […]." "The independent samples t-test showed that in terms of task completion time, there

was not enough evidence to suggest that PF icon group […] differs from NF icon group […]."

Study 2:

They "observed that participants' initial interest level toward the weather app was highly related to how much they trust the weather app […] and how much they like the weather app […]."

TRUST: The authors "found a significant main effect of privacy rating on TRUST […]. Planned contrasts revealed that a high privacy rating app […] was regarded as more trustworthy than a medium privacy rating app […]. Also, a medium privacy rating app was regarded as more trustworthy than a low privacy rating app […]." They also found "a significant interaction effect between privacy rating and framing […]." Furthermore, Bellman et al. "found a marginally significant interaction between privacy rating and presence of user rating […]. This indicates that user rating might have different effects on app's trustworthiness at different levels of privacy rating."

LIKE: The authors "found a significant main effect for privacy rating on LIKE […]. This effect tells us that how much participants liked the weather app was different for high, medium, and low privacy rating apps. Planned contrasts revealed that participants liked the high privacy rating app […] significantly more than the medium privacy rating app […]. Also, participants liked the medium privacy rating app significantly more than the low privacy rating app […]." They also "found a significant interaction between privacy rating and user rating […]. This indicates that user rating had different effects on LIKE depending on different levels of privacy rating." Furthermore, they "found a significant interaction when comparing a high privacy rating app to a low privacy rating app […]."

INSTALL: The authors "found a marginally significant association between framing and participants' choice of installing a low privacy rating app […]. The odds ratio implies that the odds of participants installing a low privacy rating app were 3.36 times higher if the rating were negatively framed than positively framed." They also "found a significant association between framing and participants' choice of installing a medium privacy rating app […].The odds ratio implies that the odds of participants installing a medium privacy rating app were 2.21 times higher if the rating were negatively framed than positively framed." Finally, they "found a marginally significant association between a user rating and participants' choice to install a high privacy rating app […]. The odds ratio implies that the odds of participants installing a high privacy rating app were 1.80 times higher if there were no user rating than the app accompanying a user rating of 3."

RECOMMEND: Bellmann et al. "found a significant association between framing and participants' choice of recommending an app with low privacy rating […]. The odds ratio implies that the odds of participants recommending a medium privacy rating app to a friend were 5.53 times higher if the ratings were negatively framed than positively framed." They also "found a significant association between user rating and participants' choice of recommending an app with high privacy rating […]. The odds ratio implies that the odds of participants recommending a high privacy rating app were 1.90 times higher if there were no user rating than a user rating of 3."

Conclusion

"Study 2 results show a strong effect of privacy rating on all dependent measures. This indicates that when a privacy rating of a given app is disclosed visually, people are influenced by the privacy rating. The influence of the privacy rating appears to decline (although still significant) when we showed a user rating of 3 […]. This suggests that people are susceptible to both privacy rating and user rating. The effect of framing was subtle." First, they "observed framing effects on TRUST in a low privacy rating app. Participants expressed a lower level of trustworthiness of an app when its privacy rating was positively framed than negatively framed. For medium and high privacy rating apps, framing effect did not occur. A similar trend was observed for INST and RCMD—a low privacy rating app was a common denominator for the framing effects to be observed, and when observed, it was always the negatively framed icons that people interpreted more positively. However, there was no framing effect on LIKE; after controlling for people's app interest level, privacy rating and user rating dominantly influenced LIKE. As we suspected, it appears that participants associated the privacy ratings with TRUST more than LIKE. Prior framing studies using text descriptions consistently show that positive framing leads to more favorable evaluations than negative framing […]. Researchers demonstrate that describing an option in a negative light […] focuses attention on the unfavorable possibilities associated with this option, rendering it less acceptable to the decision-maker […]." They "initially suspected that emphasizing negativity […] would nudge people away from privacy invasive apps with a low privacy rating. However, [the] study results suggest this is not the case. On the contrary, PF icons were more effective in making a low privacy rating app look more unfavorable." They do "suspect that people have strong connotations of 'the more, the better' in the rating context. Because a negatively framed privacy invasive app has more signs in the rating than the equivalent PF icons […] it is plausible that the higher number of ratings, regardless of its meaning, could have contributed to how people perceive the PF/NF icons." The "results also suggest that there was no framing effect in the high and medium privacy rating apps. Therefore, the use of PF icons for depicting privacy ratings is a better choice for nudging people away from privacy invasive apps while not affecting high and medium privacy rating apps."

Title	
Shining the Floodlights on Mobile Web Tracking — A Privacy Survey	
published in Proceedings of the IEEE Workshop on Web 2, 2013.	
Year 2013	Authors Christian Eubank, Marcela Melara, Diego Perez-Botero, Arvind Narayanan

Setting of the experiment

The authors design involved “porting FourthParty to Android, and driving the crawl via JavaScript […].” They conducted six “500-site web crawls through the Alexa –Top Sites in United States. Five crawls were conducted on the Android devices […] using the Firefox extension that [they] developed.” They also conducted “ a crawl using the original FourthParty Firefox extension on a PC; the date collected from the desktop crawl serves as the control for the mobile web tracking practices.” They “obtained six databases […]. All six crawls were conducted between January 21, 2013 and February 10, 2013 on the same set of 500 URLs obtained from the Alexa-Top Sites.”

The authors “ran [the] crawls using one PC, one smartphone and two tablets, as well as an emulated smartphone and an emulated tablet. They use the collected date “to survey the state of mobile web tracking in general and compare it with vanilla (desktop) web tracking.”

Research question

The authors compare “tracking across five physical and emulated mobile devices with one desktop device as a benchmark.”

Results

(copied from abstract/conclusions of the publication)

“First and third parties add more cookies on average on the desktop than on the mobile devices, which is probably due to the limited local storage on mobile devices. To [their] surprise, first-party domains on average store significantly more cookies and make significantly more JavaScript calls than third-party domains […] on every device studied […]. This reveals that the functionality of third parties is rather simple, especially on mobile platforms — each third party adds about one unique cookie. With respect to unique JavaScript calls, third-party functionality on the desktop is more complex, but the complexity decreases dramatically on the mobile devices we studied. The average top 500 third-party domain make more JavaScript calls and adds more cookies than the average third-party domain overall, which suggests that more popular third-party domains host more complex functionality.”

“An interesting implication is that the majority of third-party domains are not thought of as trackers in the usual sense […], but they nevertheless have access to protocol logs […] which frequently uniquely identify the user.” This finding leads to the question if policies or regulation on web tracking should only focus on explicit trackers, or on all third parties? “Another surprise is that the numbers are roughly the same between desktop and mobile, even though the number of JavaScript calls per domain is much higher than on desktop than on mobile […].”

Furthermore, the “dearth of third parties that exclusively focus on mobile devices is surprising. Perhaps already-established third parties have transitioned to mobile tracking or new third parties have simply not yet entered this relatively new market.”

The study also implicates that “cookies placed by third party sites have longer expiry

lengths than those placed by first party sites. As previously mentioned, while first party sites might be more likely to place at least one long-lived cookie, this log mean analysis demonstrates that, on the whole, third parties place cookies have a greater degree of longevity. Next, note that the emulated and physical phones had greater expiry lengths when compared to the desktop. The results for the two physical and emulated tablets are a bit more dispersed. A plausible reason for the increased longevity of first-party cookies on phones is that it is annoying to login on phones when a login expires. The reason for increased longevity of third-party cookies on phones is not clear."

The authors also find that […] a much larger proportion of top third-party sites place growing cookies on the desktop when compared to the mobile devices […]."

Title	
Informed Consent in Social Media Use – The Gap between User Expectations and EU Personal Data Protection Law	
published in Open access article published in SCRIPTed 435 http://script-ed.org/?p=1232	
Year 2013	Authors Bart Custers, Simone van der Hof, Bart Schermer, Sandra Appleby-Arnold, Noellie Brockdorff

Setting of the experiment

"In this paper, a set of criteria for informed consent is assessed, focusing on the question of the extent to which there exist legal provisions both in the existing and in the proposed legal framework of EU personal data protection."

First, the authors developed the set of criteria for consent that they used for their analysis. After that they conducted an online survey "regarding the awareness, values and attitudes of social media users towards privacy. The survey was comprised of seventy-five questions and subquestions covering general Internet usage, online behaviour, particularly regarding online shopping and UGCs, and the related consumer perceptions and attitudes. Attitudes and practices in the disclosure of personal data and online privacy were particularly addressed. The survey was available online between July 2011 and December 2011. A total of 8,621 respondents from twenty-six countries completed at least a part of the questionnaire. It was possible for respondents to choose not to respond to all questions in the online survey. Thus, the number of respondents to different questions varies in the results reported in this paper. […]"

"Based on the results of an extensive online survey and in-depth interviews with internet users, which were carried out in thirteen countries of the EU as part of the CONSENT project and additional literature, [they] analyzed which of [these] criteria are important to users."

Finally, "a gap analysis is made between user expectations regarding each criterion and

the availability or absence of related legal provisions in both the current and the proposed legislation."
Research question Comparison of user expectations with regard to privacy and consent when using social media with the EU legal framework for personal data protection.
Results *(copied from abstract/conclusions of the publication)* <u>Survey results:</u> „Most Internet users who responded to this survey question did not read privacy statements", mostly because they are simply too long or too difficult to understand. However, "mmost respondents (75%) sometimes, often or always watch for ways to control what they are sent online (such as tick boxes that allow opt-in or opt-out of certain offers). These results suggest that people consider such controls important.[…] [It] was confirmed by another survey question, which resulted in 82% of the respondents indicating that they "sometimes", "often" or "always" change their privacy settings when there are options available for personalising privacy settings." Also, "most respondents (73%) indicated that they never, rarely or sometimes read the terms and conditions before accepting them. When users do not read the privacy statement nor the terms and conditions, they likely do not know what they have consented to. As a result, their consent is unlikely to be strong consent […] and up to date […]." "Users show concern for privacy, although there seems to be an incongruity between public opinion and public behaviour: people tend to express concern about privacy, but also routinely disclose personal data because of convenience, discounts, and other incentives, or a lack of understanding of the consequences. […] The portion of respondents applying various security measures was on average above 50% and in some countries up to 90%. At the same time, the survey results suggested that most UGC and SNS users think it is unlikely that disclosing personal information on these websites puts their personal safety at risk." <u>Gap analysis:</u> "The proposed Regulation does contain specific provisions for parental consent […] and sets the age threshold at thirteen years old." But "that there are little or no provisions in the proposed Regulation to make this special protection more concrete." Different Articles "ask for special attention to be given to children, but none of them substantiates how this should be achieved.[…] It may be suggested that people with limited capacities to navigate and use the Internet, for instance, due to psychological disorders or limited mental abilities, may deserve special protection – similar to those afforded to children. Neither the current Directive nor proposed Regulation offer such special protection." Another thing to consider is written consent which "is not a legal requirement for consent, either in the current Data Protection Directive or the proposed Regulation.

Although this is important to users, we think the main reason for not requiring written consent is because providing consent should be technology independent. […] Nevertheless, written consent serves two main purposes: it removes the ambiguity from the consent, and it serves an evidentiary purpose. As such, in our view, written consent remains the preferred option." Although users indicated in the interviews that they considered it important to be frequently updated on policy changes […].More importantly, is that [...] users often do not have to be notified about changes in the privacy statement." This has to change as well. "Clarity regarding which data are collected, used and shared […] and for which purposes […] are important to users and sufficiently supported by the legal framework. [The authors] recommend more transparency regarding the data collected, used and shared, as most data are provided during the registration process and users may forget after some time which data they provided." "Even though most privacy statements clearly indicate user rights […], 72% of the respondents never, rarely or sometimes read the terms and conditions before accepting them, indicating that users may not be well informed about their rights. […] [The authors] recommend that user rights are also presented at the complaints site, […] However, neither the current nor the proposed EU data protection legislation provides individual users with a right to make complaints at their national Data Protection Authority." "Regarding specific and sufficiently detailed information […], users explicitly indicate that they do not want to spend much time on reading privacy statements. However, at the same time, they want to be informed properly. As straightforward solutions to this problem we suggest that information is offered in several layers, that summaries are offered and other tools are used to support the decision-making process of the consumer (such as machine readable privacy policies and visualisation tools, other than labels or icons)." "Regarding understandable information […], users indicate that they do understand the information provided in privacy statements: 63.6% of the respondents of the survey indicated that they understand the privacy statements completely or at least most part of them." Nevertheless, the authors "think legal jargon should be avoided and that the text should not be too long."

Title Data Privacy: An End-User Perspective	
published in International Journal of Computer Networks and Communications Security VOL.1, NO.6, November 2013, 237–250	
Year 2013	Authors Esma Aïmeur, Gilles Brassard, Jonathan Rioux

Setting of the experiment “This paper highlights the main data collection fields, taking a user’s view on the risks and tradeoffs regarding online data collection and privacy.”
Research question Is it possible to navigate on the web while being sure we’re not being spied on?
Results *(copied from abstract/conclusions of the publication)* “Being on the Internet implies constantly sharing information, may it be personal or not. While there are means to limit or acknowledge how much and what we’re sharing, many agrees that the current situation is unbearable. To counter this phenomenon, there are various privacy enhancing technologies that may be used, but they will never be sufficient because re-identification is always looming. We’re facing a unique, uncomfortable situation: as social media is booming and more and more people are using the web to share information, privacy issues are becoming more complicated, yet increasingly important. The digital economy is changing at an everincreasing pace. Being connected is now fundamental for many individuals, and companies are tapping into that market: Google is now trying to change the Internet providers’ market by launching Google Fiber8 in selected cities, an obvious move considering the nature of their business. The more often people are online, the better the outcomes for those digital conglomerates. We know that collecting, aggregating and using data is the backbone of the Internet: search engines, banking websites, credit rating agencies, caching and archiving services, those platforms are more data-driven than ever before. Every person connected on the Internet takes the role of the enduser one time or another. Is it worthwhile to try to keep decent privacy online? “Digital Natives”, [...] do not really care about disseminating their information. Even if they are wary of the consequences, they claim that life is for sharing! ‘They want to be the targets of marketing. They want their data shared. They want to get catalogues mailed to their homes. They want to be tracked. They want to be profiled.’ Is it because we are not sufficiently aware of the implications? Is it because the advantages outweigh the inconveniences? Although an imperfect analogy, we consider that thinking in terms of a “Digital Wallet” that would contain our private information is a powerful image to convey the importance of privacy. As a real wallet contains (beside cash) precious information that could be dangerous in the wrong hands, a digital wallet, improperly secured, can lead to undesirable consequences to one’s online experience. Privacy, and more specifically online privacy, seems like a zero-sum game: we’re trading privacy for convenience or better information. Is it now too late to combine the better of both worlds? Are we sufficiently aware of the consequences of our online actions? Knowledge is power: did we let some entities become too powerful?”

Title A Review of Consumer Information Remedies	
published in Research Document, 12th March 2013 http://stakeholders.ofcom.org.uk	
Year 2013	Authors Ofcom
Setting of the experiment Ofcom "carried out a series of interviews with stakeholders in order to inform [their] review, but have also compiled findings from published research, including academic studies." They have also "worked with I2Media Research in compiling the desk research and with Stephen Locke, an independent expert in consumer policy, who peer reviewed the report and contributed to the examples of current practices."	
Research question This paper is designed to provide a review of the use of information remedies as a consumer protection and empowerment tool.	
Results *(copied from abstract/conclusions of the publication)* "Ofcom's starting point is that well-functioning markets tend to deliver good outcomes for consumers." Information remedies are measures "to solve […] a market problem by providing information to consumers, with the aim of helping them to make informed decisions about products and services." But when assessing the potential of information remedies, there are some facts that need to be considered: Behavioral tendencies: "[…] consumers do not always operate according to standard economic theory, which assumes that consumers make simple rational choices. […] The way in which information is framed […] can affect consumers' responses to it, to the extent of making poor decisions. […] In some instance, concerns about the behavioral tendencies have contributed to policy decisions not to rely solely on an information remedy […]." Ofcom found that "information may have less impact and so need careful consideration where consumers' attitudes, understanding or behavioral tendencies present barriers to them engaging with and action on the information." Characteristics of information provision: awareness, accessibility, trustworthiness, accuracy, comparability, clarity and understanding, informational design, timeliness The authors "desk research identified very few research studies that have evaluated the effectiveness of regulatory information disclosure. […] However, one academic paper from the United States assesses the effectiveness of such transparency systems by examining the design and impact of financial disclosure, nutritional labelling, workplace	

hazard communication, and five other systems. It emphasises the need to consider the information users' needs, the context in which they operate, and the available options and costs for obtaining information. It concludes that transparent information provision is only effective '*when the information they produce becomes 'embedded' in the everyday decision-making routines of information users and information disclosers*'. [72] The paper identified this as a critical condition for the effectiveness of an information remedy. Although, as discussed earlier, it is not always necessary for all consumers to understand and act on information, but if a sufficient number do, it can have a disciplining impact on the market."

"Evaluation of the effectiveness of information remedies is therefore very much in its infancy as a subject. However, from the areas [Ofcom] have studied from this project, [they] suggest the following provisional checklist […].

- Is consideration given to evaluation objectives and metrics early on in the process when designing the information remedy?
- Are sufficient resources and time available for the collection of data and the completion of the evaluation stage?
- Are the objectives of the information remedy sufficiently clear, for example in terms of the target group of consumers and the required impact?
- Is there a clear benchmark; for example, in terms of consumer knowledge, attitude and behaviour, against which any subsequent changes can be measured?
- Is a single metric sufficient or will a suite of measures be more useful?
- Are the methods proposed for the collection of data appropriate to the target group and to the initiative under evaluation?
- If sufficient direct evidence, for example of changing consumer behaviour, is not available, is any proxy evidence needed?"

Title Automated Text Mining for Requirements Analysis of Policy Documents	
published in Requirements Engineering Conference (RE), 2013 21st IEEE International, pp. 4-13	
Year 2013	Authors Aaron K. Massey, Jacob Eisenstein, Annie I. Antón, Peter P. Swire
Setting of the experiment The authors perform "a large-scale analysis of 2,061 policy documents". Including policy documents from Google Top 1,000 most visited websites and the Fortune 500	

companies […].” They also uses a set of policy documents which from one of their prior analysis on financial privacy policies.

For each data set from the three different sources, they “visited the homepage for each website and manually collected any policy documents for each organization. These policy documents included Privacy Policies, Privacy Notices, Terms of Use, Terms of Service, Terms and Conditions, and similarly titled documents.”

Methodology

The authors “analysis methodology consists of three steps: (1) readability analysis of policy documents, (2) building and validating a topic model of the policies, and (3) exploring privacy protection goals and vulnerabilities using the topic model.”

The readability of policy documents is measured by using five metrics: “Flesch Reading Ease, Flesch Grade Level, FOG, SMOG, and the Automated Readability Index (ARI).”

“Probabilistic topic models are designed to uncover the hidden themes in large document collections that would otherwise be impossible to analyze through human annotation. […] The particular topic modeling algorithm [they] apply […] is the Latent Dirichlet Allocation algorithm […].”

Research question

“Regulators, consumers, and requirements engineers share an interest in the content of policy documents, but there are few tools to assist in their analysis of these documents.” The author “present a methodology for analyzing the requirements specified in 2,061 policy documents” in addressing 3 research questions:

1. “How similar, with respect to readability, are policy documents of different types, organizations, and industries?”
2. “Can automated text mining help requirements engineers determine whether a policy document contains requirements expressed as either privacy protections and vulnerabilities?”
3. ”Can topic modeling be used to confirm the generalizability of the Antón-Earp privacy protections and vulnerabilities taxonomy?”

Results

(copied from abstract/conclusions of the publication)

Readability results:

The results indicate “that policy documents [are] extremely difficult to read. Both the Google Top 1,000 and the Fortune 500 policy documents are rated more challenging to read than the policy documents in the first two studies. This may be the result of regulatory influence in the five years” since their last study was conducted. The implications of this results are that “requirements engineers need tools and techniques to analyze these documents and ensure that software deployed by organizations lives up to the promises in their policies. Official policy documents should reflect an organizational commitment and serve as a mutually understandable agreement

between the organization and the consumer. The challenge of interpreting these policies does not fall on requirements engineers alone. Regulators and customers also need to evaluate and understand these policies. Even if these policies were easily readable and coherent, which is clearly not the case, the sheer number and length of policies would remain an obstacle to overcome. For all of these reasons, we believe the use of text mining techniques, which can improve and augment both requirements engineering analysis and regulatory understandability, are justifiable and worthwhile pursuits."

Topic Model:

Our results demonstrate that policy documents are similarly challenging to read and understand [Question 1]. Additional tools and techniques are needed to support the software requirements engineers building systems that must uphold the promises these documents make to end users. The results of [their] work also indicate that topic models can indicate whether a document contains software requirements expressed as privacy protections or vulnerabilities [Question 2]. These requirements have serious implications for requirements engineers or regulators seeking to build or evaluate software systems that must comply with these policies. Clearly, topic models cannot replace requirements engineering analysis conducted by trained individuals. Applying the heuristics needed to extract goals from these documents requires trained engineers. This matches the common understanding that natural language processing techniques are not capable of specifying software requirements. Finally, [their] results provide preliminary support for the generalizability of the Ant´on-Earp taxonomy to multiple domains [Question 3]."

Title	
Form Matters: Informing Consumers Effectively	
published in	
Amsterdam Law School Legal Studies Research Paper No. 2013-71	
Year	Authors
2013	Natali Helberger

Setting of the experiment

The author provides a theoretical study about consumer information. "Consumer information has an important function in correcting information asymmetries, and in enabling consumers to make transactional decisions that respond to their individual preferences and requirements." Additionally, mandated consumer information is perceived as a " less intrusive form of government interference, one that leaves the autonomy of market players in principle intact and refrains from imposing mandatory standards of consumer protection that either hinder market developments and innovation."

But “informing consumers does not automatically result in informed consumers […] it is not only the content of information that matters, but also […] the form in which it is presented and communicated to the consumer.” Form aspects, however, has been neglected in former studies. “Effective communication of consumer information is key in an increasingly complicated and abundant ‘information economy’. It is also a question that general consumer law and policy has still largely neglected, but can no longer afford to do in the future.”
Research question The focus of this research paper is the effective communication of consumer information. The study concentrates “on the communication in terms of use and contract terms”.
Results *(copied from abstract/conclusions of the publication)* „Transparency and informed consumers are […] the result of complex processes in which a variety of different actors and factors are potentially involved. Placing consumer information in its broader perspective is not only important for the decision whether, and if so, which information to make mandatory, but also: in which form.” But there are a variety of “behavioural restraints that effective communication of consumer information needs to overcome”. This following cognitive failures and biases affect “the form in which consumer information must be delivered in order to be communicated effectively”: 1. “consumers are unaware of and/or do not read consumer information or contract terms” 2. “they do not understand or misinterpret what they have read” 3. “they fail to act as the regulator expected them to react” 4. “they fail to notice and consequently adapt their choices to newly received information” In order to circumvent this obstacles and “to be effective, consumer information must be framed and communicated in a form that is actually useful and effective for consumes.” Consumer information should therefore create awareness, be easy to access and well-timed. The latter means that “consumers should ideally be presented with information (and only the information) that they need at the moment when it is relevant.” Also “the form in which information is being presented matters.” Finally,” consumer information […] must be presented in a form and in a context that allows consumers to make a link with their actual situation, their information needs and experiences.” To further improve the presentation of consumer information the amount of information has to be reduced. “This study has argued that piling ever more information on the consumer without having measures and safeguards in place that guarantee that consumers are given the chance to engage meaningfully with that information is

ineffective and creates a false sense of security and trust. It also creates the illusion of 'consumer empowerment' in situations where too much or badly presented information rather does the opposite: it confuses and weakens the consumer's position in the market. Consumer information may be a powerful tool, but only after substantial effort has been invested not only in making that information available, but also in communicating that information effectively."

The author concludes that "a key to understanding the conditions for the effective communication of consumer information is to realize that consumer information is not a one-time act, it is a process. This process involves different stages of processing information: becoming aware of the information, collection and processing of consumer information, acting upon it and staying up to date. At each of these stages consumers can have different information needs, and may need information in different formats and functions. Eventually, the same items of information would need to be repeated for the different steps. […] At a minimum, consumer information should be communicated in comparable and ideally standardized and machine-readable format. It would need to be written from the perspective of consumers, and not lawyers, and offer explanations of the (legal) concepts used as well as real-life implications."

Title Smarter Information, Smarter Consumers	
published in Harvard Business Review, January-February 2013	
Year 2013	Authors Richard H. Thaler and Will Tucker
Setting of the experiment This article analyses opinions and ideas about the new changes in technology and disclosure rules.	
Research question "Changes in technology and disclosure rules will help shoppers make better decisions."	
Results *(copied from abstract/conclusions of the publication)* Consumers are „influenced by all sorts of superficial things, and they procrastinate and don't read the small print. You've got to create situations that allow them to make better decisions for themselves." "Unfortunately, disclosure and regulatory policies have generally been written with the implicit assumption that as long as the costs of obtaining information are relatively low, the structure and format of disclosure are relatively unimportant. The burden of	

deciphering and understanding disclosed information is left to consumers.

"Smart disclosure falls into four broad categories: (1) government release of data it collects on products and services; (2) government release to individuals of their personal data (such as Social Security contributions and tax returns); (3) government-facilitated electronic disclosure by private sector companies of price or attribute data on products and services; and (4) government-facilitated release to consumers of personal data held by the companies providing the products and services."

"The key is to use data to empower consumers via smart disclosure. Smart disclosure alone won't make people better decision makers – but it will get machines and complex options working for consumers, just as big data can help companies improve business strategy. This policy innovation has the potential to be a win-win-win: Consumers can win by getting the products and pricing plans that best suit their preferences, essentially reducing their cost of living. Businesses can win by competing on high-quality products at good prices, without the risk of losing out to less scrupulous firms that compete through deception. And entrepreneurs and innovators can win by devising new ways of serving consumers."

"The rise of choice engines will do more than create super shoppers. It will make markets more efficient, create new businesses, and improve the way governments serve their citizens."

Title Smart Disclosure and Consumer Decision Making: Report of the Task Force on Smart Disclosure	
published in https://www.whitehouse.gov/sites/default/files/microsites/ostp/report_of_the_task_force_on_smart_disclosure.pdf	
Year 2013	Authors Executive Office of the President National Science and Technology Council (USA)
Setting of the experiment The report "was developed by the Task Force on Smart Disclosure: Information and Efficiency in Consumer Markets […] under the National Science and Technology Council's Committee on Technology. " This report "marks an important milestone for the Administration's policy of liberating data for the benefit of the economy and society – a policy that was strengthened and codified in May, 2013 […]."	
Research question "(…) comprehensive description of smart disclosure approaches being used across the Federal Government. It provides an overview of the ways in which smart disclosure can	

empower consumers and increase market transparency; describes smart disclosure activities being undertaken by Federal agencies and partners; provides context about government policies that guide and support those activities; and presents examples of concrete steps already being taken by Federal agencies to advance smart disclosure in domains such as health, education, energy, finance, and public safety."

Results

(copied from abstract/conclusions of the publication)

"Smart disclosure empowers consumers to make better-informed decisions when facing complex marketplace choices. […] it can be difficult for consumers to identify the product or service that best suits a particular need. In some cases, the effort required to sift through all the available information is so large that consumers default to decision making based on inadequate information. As a result, they may overpay, miss out on a product better suited to their needs, or be surprised by fees." Smart disclosure also give consumers "access to useful personal data; power new kinds of digital tools, products, and services for consumers; and promote efficiency, innovation, and economic growth."

The Federal Government's tasks in expanding the use of smart disclosure are to "are to improve and promote access to smart disclosure data; […] [to] encourage sellers to make more information about their products and services directly available to the public; […] [to] make the personal data they collect securely available to the individuals to whom the data pertain; […] [to] create its own consumer-facing choice engines that use smart disclosure data. " The Federal Government already took some necessary steps to promote smart disclosure across sectors such as education, energy, finance, food, health care, safety, telecommunication, transportation.

Integral to effective smart disclosure are strong privacy protections. "The privacy issues that arise in the context of smart disclosure are different depending on the type of data concerned. In some cases, smart disclosure data is not related to specific people, such as when agencies publish information on the prices of consumer services or the locations of companies. Such cases may not implicate privacy issues. […] in some cases, smart disclosure involves providing personal data to the authenticated individual to whom the data pertains. In these cases, agencies must ensure strong privacy and security safeguards are in place to ensure that the data is made available only to the authenticated individual."

The authors also point out, that "poorly organized or inaccessible information can also make consumer markets less efficient, less competitive, or less innovative."

Finally, the authors provide two recommendations:

1. "Agencies should incorporate smart disclosure as a core component of their efforts to institutionalize and operationalize open data practices."
2. "Develop a government-wide community of practice."

Title Do online privacy policies and seals affect corporate trustworthiness and reputation?	
published in International Review of Information Ethics 19(7): 52- 65.	
Year 2013	Authors Orito, Y.; Murata, K. and Fukuta, Y.
Setting of the experiment "The questionnaire survey was conducted in May 2013 using the online questionnaire website. The respondents were university students [...]." The follow-up interview is mainly conducted to answer the following question: "Why do the respondents not read privacy policies but yet they believe that companies comply with online privacy policies when they shop online?" "The questionnaire's title was 'Online Shopping Survey 2013', and at the start of the questionnaire it included an explicit statement - 'The aim of this survey is to analyse online shopping behaviour' - to avoid priming. Tendencies of and relationships between responses to the questionnaire were examined through statistical tests […]. "	
Research question Examination of the "effectiveness of online privacy policies and privacy seals/security icons on corporate trustworthiness and reputation management" and clarification of "how young Japanese people evaluate the trustworthiness of B to C e-business sites in terms of personal information handling."	
Results "[…] more than 80% of respondents knew of the existence of online privacy policies" and "the proportion of respondents who considered an online privacy policy as an important element for their online shopping […]." Nevertheless, "the results of the survey […] indicate that more than half of the respondents who acknowledged the importance of online privacy policies when they purchased something online did not actually read the policies frequently." "Moreover, it seems that their recognition of the importance of online privacy policies is not necessarily relevant to their practical concerns about online privacy policies. […] it is notable that more than half of these respondents answered that they rarely worried or did not worry about companies' compliance with online privacy policies. That is, even among the respondents who recognised the importance of the policies, the majority of them did not worry about whether online shopping companies actually complied with their online privacy policies." Furthermore, the "survey results show the tendency that over three-quarters of the respondents […] believed that companies did comply with their privacy policies […]. Although the proportion of respondents who do not read online privacy policies was	

highest, many of them seemed to believe that many companies did comply with their online privacy policies […]. Thus, regardless of their recognition of the importance of online privacy policies, or whether they had read online privacy policies, it seems that the majority of respondents believed companies did comply with online privacy policies without any reasonable ground or clear evidence for it."

The study also revealed that the "proportion of the respondents who understood the encryption of personal information during transmission was over half (55.9%). […] It appears that the respondents' recognition of encryption technologies was not very high. Additionally, many respondents did not understand the meaning of privacy seals and security icons […]."

Finally, after evaluating the characteristics a website needs to have in order to provide personal information, it "is easy to see that many respondents used name recognition of the websites or their operators rather than the implementation of privacy protection schemes, as a standard to evaluate the trustworthiness of B to C e-commerce sites in terms of personal information use and protection. Additionally, over half of the respondents did not want to provide information to websites that have suspect web designs and too many advertisements; such websites may have a disadvantage in some cases, even if they earnestly work to establish appropriate privacy protection schemes. If the most important factors for cultivating consumer trust in online businesses are name recognition and the reputation of websites and/or their operators, it would seem that the efforts of companies in terms of online privacy protection alone are not rewarded."

Conclusion

" […] it cannot be said for sure that posting online privacy policies and privacy seals/security icons on online shopping websites is working to engender trust and enhance the reputation of online shopping websites in a proactive manner. Rather, the existing name reputation of online shopping websites, the general reputation of the business organisations operating online shopping websites, and ease of access to reputational information can contribute to engendering a sense of trustworthiness and a better reputation in terms of personal information use and protection."

2014

Title	
An Exploratory Survey of the Effects of Perceived Control and Perceived Risk on Information Privacy	
published in 9th Annual Symposium on Information Assurance (ASIA'14), June 3-4, 2014, Albany, NY: 23-28.	
Year 2014	Authors Clare Doherty, Dr. Michael Lang
Setting of the experiment "An on-line survey comprising 24 questions […] was administered to a sample of internet users based in Ireland. 260 usable responses were received." "The questionnaire items captured data about: (1) general demographic variables; (2) attitudes towards online privacy; and (3) perceived online risks, safeguards and controls. Convenience sampling […] was used as the sampling technique. Participants were solicited through personal messages sent via LinkedIn, Twitter, and Facebook." The "population of interest was not the general public as a whole but rather those who have some level of awareness of online privacy issues, the use of social media to attract respondents and the use of a Web-based instrument to collect data are methodologically justifiable." Demographics of respondents included the age ranging from 17 to 61, with a mean of 29 years. 60% of respondents were females, 73% of respondents were employed and 82% of respondents were of Irish nationality. The survey data was analyzed in the statistical software package SPSS running descriptive statistics tests, Cronbach's Alpha estimate of reliability test […] and non-parametric tests of correlation[…]."	
Research question How does "perceived control and perceived risk affect information disclosure"?	
Results *(copied from abstract/conclusions of the publication)* <u>Perceived Control</u> "40% of respondents feel they have little or no control over who can view their online information while 66% of respondents indicated that they feel uncomfortable about their personal data being in the control of others. In relation to users' perceived ability to exert control over how their online personal information is used, 84% believe they have little or no control over the actions of other users while 60% of respondents feel that they have little or no control to correct inaccurate or untruthful information about themselves. An overwhelming 81% of respondents feel they have little or no control over 'their ability to prevent their data and actions from being used or analyzed by online companies in ways they did not intend'."	

"Non-parametric correlation tests were also run and it was found that the less control a person perceives themselves as having over their privacy online, the more uncomfortable they feel about information being in the hands of others […]. As expected, those who feel they have the least control are also the most concerned that other internet users might abuse their personal information […] and that online companies might divulge their information to other parties without explicit consent […]. The level of an individual's perceived control over privacy is also correlated with the amount of information they choose to disclose. The more information they reveal, the less control they feel they have over their ability to prevent their data from being used by online companies in unintended ways […].This is interesting because it suggests that people are giving away their information in the knowledge that they are sacrificing control. It may be that they are happy to do so in the expectation of receiving enhanced online services on the basis of "value exchange" […] in which they feel compelled to do so in order to avail of fairly normal functionality, i.e. a trade-off. In relation to a user's perceived level of control and the incidence of adverse experiences, the more control that respondents feel they have over their online privacy, the less often they have ever been the victim of online fraud […] or had an unpleasant experience as a result of online disclosure […]. This finding might be interpreted in two ways; it may be the case that some persons feel they are in control because they have not yet had a bad experience, or they may indeed be in control as a consequence of which they have not suffered a breach. However, our respondents overall, feel they have little control over their information once it is disclosed online."

Perceived Risk

"32% of respondents disclose nothing or only a small amount of personal information, with a further 58% stating they disclose 'only what I have to'. 74% of respondents either agreed or strongly agreed with the statement 'I tend to reveal minimal personal information about myself online because I value my rights to privacy' as to why they withhold information. Those in the age category 33+ are considerably less bothered about potential damage arising from their information being 'Accessed by someone you don't want […]' or 'Used against you by someone […]'. This may be because they tend not to disclose as much information online as younger age groups. 50% of respondents believe that something unpleasant might happen to them due to their presence on the internet."

"As regards adverse online incidents, 39% had been subjected to privacy violations of some kind, while 20% indicated that their personal reputation was damaged as a result of material posted online. 50% of respondents feel they are not at all protected against damages to their reputation caused by online companies as a result of information disclosed. It is increasingly the case that employers are looking at the online profiles of prospective employees. Therefore, if users partake in risky behavior and it is revealed online, there is the possibility this will affect an aspect of their life for example a relationship or their career. Respondents in this study were in favor of the view that persons should not always be judged on the basis of past behavior (68%). Interestingly 25% of respondents believe it depends how long ago the material was posted online,

that users should be held accountable for their actions for a certain amount of time. Non-parametric correlation tests […] were run and it was found that users perceive it risky to disclose information online as they feel uncomfortable about their personal information being in the hands of others […] which reflects possessing a low level of trust. The more often online information is used for commercial purposes; the greater the risk their online accounts will be maliciously accessed by an unauthorized person thus users possess a greater level of trust in people they know than in online companies. A person's privacy online is subject to greater threat due to the risk of other internet users abusing their personal information […]. The more information that is disclosed online by a user, the greater the chance that the privacy of their online information will be violated […]."

Conclusion

"This study has demonstrated that our respondent's privacy concerns of perceived control and perceived risk determines how much information they reveal. In general they do not feel in control over the information they disclose online and they possess a greater level of trust in people they know online rather than online companies. The majority of respondents stated they only disclosed information online that they were required to; however, some respondents were still subject to privacy violations and reputation damage. Respondents also feel they are at risk due to their online presence and disclosing their information online."

Title
What do they know about me? Contents and Concerns of Online Behavioral Profiles
published in
Conference paper: PASSAT '14: Sixth ASE International Conference on Privacy, Security, Risk and Trust, At Cambridge, MA, December 14-16, 2014

Year	Authors
2014	Ashwini Rao, Florian Schaub, and Norman Sadeh

Setting of the experiment

To understand contents and concerns of behavioural profiles, Ashwini et al. "first conducted semi-structured interviews in which [the authors] asked [their] participants (n=8) to look at their own profiles." After that, they "conducted an online survey (n=100) to confirm that [the previously] identified user concerns with a more diverse audience."

Interview

From those interviews, the authors "gathered and categorized the information overserved in the behavioural profiles of [their] participants." During the interviews, they "also elicited participants' concerns and surprises regarding information in their profiles."

The authors "studied behavioural profiles from three companies: BlueKai Registry,

Google Ad Settings, and Yahoo Ad Interests." All these are cookie-based profiles.

The authors conducted "semi-structured in-person interviews with eight participants." The participants were "graduate students with engineering and/or science background." The authors started explaining them "that companies may collect data about them, and may create behavioural profiles." The author also informed the participants "that they might be able to access their profiles" and "requested them to look at their profiles (BlueKai, Google, and/or Yahoo)", and share information with the authors if they felt comfortable." Actually 7 of 8 participants showed the authors content from their profiles.

Survey

The survey was designed to achieve two goals. First, they "wanted to confirm whether a more diverse population of users agreed with the concerns that [they] had identified from the interviews." Second, they "wanted to identify additional user concerns."

The authors "recruited participants (n=100) from Amazon Mechnical Turk crowd-sourcing platform." Their "participants were at least 18 years of age and located in the United States." They got compensation.

To understand whether the [100] survey participants agreed with the concerns that the authors identified from the interviews. The authors used a sample profile to understand the participants' concerns regarding collection of sensitive data, amount of data, combining data from multiple sources, level of detail and data use.

The authors "created the sample profile using data from profiles of the interview participants." After showing them the sample profile, the authors "asked them to select, from a list of six items, at least two items present in the sample profile. [The authors] then asked the participants to rate, on a 5-point Likert scale of "Strongly disagree" to "Strongly agree," how much they agreed or disagreed with the following list of concerns. We randomized the order in which the concern statements were displayed.

1. I am concerned because I believe that the profile contains sensitive data
2. I am concerned by the amount of data in the profile
3. I am concerned because my data from multiple sources (e.g. online activities, in-store, other companies) is being combined
4. I am concerned by the level of detail (e.g. specific information, not just broad categories) in the profile
5. I am concerned about how my data may be used

Research question

Investigation of behavioural profiles of users by utilizing access mechanisms given by companies to access behavioural profiles

Results

(copied from abstract/conclusions of the publication)

Interview

Two Google profiles ~120 items, one Yahoo profile had ~25 items, one BlueKai profile had ~10 items, two BlueKai profiles had ~30 items, and two BlueKai profiles had ~570 items.

For further investigation the Ashwini et al. "organized the date from these profiles into seven categories: demographic, geographic, technical, predictive, psychographic, behaviour and life event."

"Participants expressed […] concern about credit and health information." one participant who has an extensive profile with ~570 items was surprised and concerned by the amount of data gathered. […] Further, he was concerned to see his data from multiple sources being combined. […] One participant was okay with broad interest categories, but not with specific categories. […] Participants were concerned about how the data in their profile may be used. […] In general, participants were not concerned when the data was incorrect. […] Participants, however, became concerned when the data in the profile was correct."

Survey

For each of the five concerns, at least 70% of the participants either agreed or strongly agreed that they were concerned. Participants were most concerned about how their data may be used (85%), followed by level of detail (77%), aggregation (75%), amount of data (73%) and collection of sensitive data (73%). Seven participants were concerned about the security of their data; they worried that their data could be abused by hackers, criminals and identity thieves. Four participants expressed concerns that their data could be shared or sold to third parties, and accessed by the government. These are important and should be explored further. Fifty participants agreed (17 strongly agree, 33 agree) that their liking for personalization had decreased after seeing the types of data collected for personalization, and 23 disagreed (2 strongly disagree, 21 disagree). Interestingly, 18 of those 50 participants were participants who liked personalization of ads. Seventy one participants (71%) chose to look at their own profiles even when it was optional. This indicates that people are interested in learning about their behavioral profiles. This may also indicate that many people are unaware of profile access mechanisms provided by companies. This is similar to [the] interview pool where only one out of eight participants was aware of profile access mechanisms. Out of 71 participants, 51 (72%) chose to report their reactions. [The authors] analyzed their comments for concerns regarding accuracy and editing profile data. Nine participants (17%) reported empty profiles. Twenty three participants (45%) reported inaccuracies, and only three participants (6%)) reported that they found accurate profiles. Participants' reactions to inaccuracies included "blatantly incorrect," "80% inaccurate," "somewhat dated" and "hilariously overestimated." Recall that all [the] interview participants had also found varying levels of inaccuracies in their profiles. Most of the participants who reported inaccuracies and empty profiles explained that they felt relieved and less concerned about data collection. Only two participants (4%) felt that inaccuracies in their profiles could adversely affect them. Three participants mentioned about editing data. One of them corrected errors, and two of them deleted correct entries. Reactions of survey participants regarding inaccuracies in profiles and

editing profile data appear similar to those of interview participants. During analysis of participant reactions, we did not find any new data types. Lastly, [the authors] looked for comments that signalled difficulty in comprehending profile information. One participant explicitly reported not being able to understand parts of his BlueKai profile. Two participants thought "High/Medium Confidence" was referring to their personality. Some of our interview participants had similar difficulties. Overall, [the] survey results confirm the results from [the] interviews."

The authors' "study shows that a large number of behavioral profiles contain inaccuracies. All interview participants (8/8) and 45% (23/51) of survey participants, who provided feedback about their profiles, reported errors. This violates an important fair information practice principle: the data quality principle. Although companies seem to be verifying the accuracy of the data that they obtain, it is not clear how effective their processes are. Since data is being combined from multiple companies, a few companies taking steps to ensure correctness may not be sufficient."

"Users would benefit if companies that create behavioral profiles provide better notice about collection, combining and potential uses of user data. Improving awareness of access mechanisms among users can also help users. At present, there seems to be little awareness, for example, only one out of eight interview participants knew about access mechanisms. Users would benefit if companies get users' consent before combining data from different contexts. To alleviate users' concerns regarding data use, companies could disclose the purposes for which they use profile data. Further, they could specify what inferences they draw and how their prediction models work. From a user's perspective, stating that the company uses proprietary models, for example, "developed a proprietary algorithm that utilizes a consumers name, mailing address and 320 different data points to accurately assign a personality type to 85% of US adult consumers," may be insufficient. To address user concerns regarding level of detail of profile data, companies could explain the need for such level of detail. Lastly, users would benefit if companies ensure accuracy in profile data and address the issue of accountability for adverse impact arising from errors in profiles."

Title	
Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts	
published in	
The Journal of Legal Studies, Vol. 43, No. 1 (January 2014), pp. 1-35	
Year	Authors
2014	Yannis Bakos, Florencia Marotta-Wurgler, David R. Trossen
Setting of the experiment	
Bakos et al. "track 48.154 visitors to 90 software companies over a period of one month [in January 2007], recording their detailed browsing behaviour."	

Their final data "includes detailed demographic characteristics of each user, such as age, gender, income, and geographical location." For example, "the average age of the users […] is 46, and the range is reportedly from 18 to 99." For each user they also "observed the exact sequence of web pages (URLs) accessed in a particular visit and the time spent on each website. " After excluding all the companies for which they do not have enough date or otherwise are inappropriate for their tests, they arrive at a final sample of 90 companies, as mentioned above. For further investigation they divided these companies into two types of software companies: retailer and freeware providers. Their final sample, therefore, consists of 78 retailer and 12 freeware companies. "All else being equal, consumers may feel less need to scrutinize the terms in EULAs from companies that are large or old because they assume that such companies are more trustworthy and fair. To test this hypothesis, [they] obtain information about each company's annual revenue, year of incorporation, and public or private status. These data were obtained from Hoovers.com, Yahoo! Finance, or via direct communications with the companies in the sample." Finally, "in order to empirically investigate the existence and size of the informed minority, [the authors] classify visitors to the websites of the companies […] into potential buyers and those visiting for other reason." They "use access to a EULA page for more than one second to identify readers."
Research question Does an informed minority of buyers capable of disciplining the market actually exist?
Results *(copied from abstract/conclusions of the publication)* <u>Results</u> "Looking at uninterrupted session/visits […], under the least strict definition of a visit (2 or more pages accessed), there are 131,729 such visits to software retailers and 28,663 to freeware providers, including repeat visitors. For retail companies, an average visit consisted of 12.1 page views over 303 seconds (5.05 minutes). These numbers, however, are driven by extreme values. The median number of pages visited in any given company is 5 and the median time spent is 101 seconds (1.68 minutes).The data indicate that EULAs were accessed in only 63 of the 131.729 visits to software retailers (00,5% of all such visits) an in 44 visits to freeware companies (0.15%). Users that accessed EULAs in retail companies visited an average of 19,1 pages […] in that company's site prior to the EULA page. […] the average time on the EULA page was 59,4 seconds and the median time was 34 seconds. […] Forty-six of these accesses were less than 30 seconds, and 92% were less than 2 minutes. […] the time spent in the EULAs relative to their length indicates that most readers did not read terms in their entirety, especially as they are generally written in complex legalese and since consumers are unlikely to be aware of the default rules, even if EULAs do spell out some terms in clear language, there is still a likelihood for misunderstanding. […] Visitors to freeware providers have a mean of 13.4 pages view […] and are of shorter

duration (median time spend is 43 seconds). This is expected, as freeware sites tend to be sparser. EULAs are accessed in 0.15% of these visits. The median time spent on EULAs is a similar 33.5 seconds with 50% under 30 seconds and 86% under 2 minutes […]. "

"When a visit is defined to require five or more pages accessed at the company visited, there are 72,282 uninterrupted session/visits to software retailers and 13,715 to freeware companies. The median number of pages viewed in a given visit to a retailer is now 10 pages and the median length is 183 seconds (3.05 minutes). Distributions of page views and duration are again skewed. EULAs were accessed at a slightly higher rate in these visits, 57 times among software retailers (0.08%) and 30 visits among freeware companies (0.22%). The median number of pages seen before accessing a EULA was 8 for retailers and 4 for freeware providers. Times spent on EULAs are similar as before, with about half the accesses under 30 seconds and 90% under 2 minutes."

"Finally, limiting our consideration to visits to software retailers that included initiation of a secure checkout session, the number of visits falls to 4,866, with 5 median page views per visit, but longer mean and median durations. This is expected since purchases require more time to process the transaction. In this restricted sample, there are 7 voluntary accesses of a EULA in the course of purchase, constituting 0.14% of all visits. All accesses are at least 30 seconds, and the median time spent in the EULA almost doubles for users in this group to 60 seconds. Interestingly, out of all sessions with EULA visits, 3.7% (if we use the two page visit definition) or 6.7% (if we use the five page visit definition) resulted in initiating a checkout session. If all of the initiated checkout sessions were completed leading to a purchase, the resulting conversions would be significantly higher than the typical 2% conversion rate in Internet purchases."

Conclusion

They "find that very few consumers choose to become informed about standard form online contracts. In particular, [they] estimate the fraction of retail software shoppers that accesses EULAs at between 0.05% and 0.22%, and the very few shoppers that do access it do not, on average, spend enough time on it to have digested more than a fraction of its content. [They] also document that shoppers rarely access other substitute information sources, such as consumer product review or relevant news sites, to learn about EULA terms. Even under generous assumptions, it is hard to envision the probability that EULAs are read, and understood, growing even to 1%. [Their] estimates of the size of the informed minority in this market are one or two orders of magnitude smaller than examples offered in the literature for the size required to sustain an informed minority equilibrium […]." Furthermore, "such a small number of contract readers would seem to cast doubt on the existence of an informed minority of a size sufficient to police against one-sided terms, at least in the context of software sold online."

In general, "shoppers are more likely to access the EULAs of smaller companies or companies that offer ex ante somewhat suspicious products such as freeware. The few

shoppers that choose to become informed might be rationally deciding to ignore the EULAs of larger, more established companies, relying instead on company reputation or familiarity. [They] also find that older and higher income shoppers are more likely to access EULAs; this may be because these consumers have lower search and reading costs, e.g., because they have a lower opportunity cost for their time or because they are more educated and thus find it easier to read contract terms. Thus, although only a tiny fraction of consumers read unconditionally, the fraction grows a bit when expected benefits are likely to be higher or costs are likely to be lower; thus consumers seem to behave at least directionally in accordance with search theory, suggesting that the lack of a significant informed minority is due to high search and reading costs of standard form contracts."

Title Participatory Transparency in Social Media Governance: Combining two Good Practices	
published in Journal of Information Policy, Vol. 4, 2014, pp. 529-546	
Year 2014	Authors Stephan Dreyer, Lennart Ziebrath
Setting of the experiment "The article analyses theoretical scenarios of […] participatory transparency – i.e. ways in which users participate in improving transparency, and their respective advantage and drawbacks."	
Research question Exploration "the potential of community-based bodies in the field of social media governance for […] improving transparency [of] Terms of Service and Privacy Policy"	
Results *(copied from abstract/conclusions of the publication)* "In the area of social media governance, participatory transparency is one option, for improving transparency for users. By discussing terms and Policies as well as illustrating their meaning and consequences, users can be made aware of the mere existence of such provisions and of how relevant issues they are for their own informational privacy. User participations to solve transparency-related issues, for instance, could consist of users pointing out insufficient legibility or comprehensibility of the Terms and Policies or part thereof. Such participation may also include identifying problematic cognitive dissonance regarding the users' expectations and the actual content and provisions of a platform's policies. Moreover, participatory transparency can function as a trustworthy way to align platform provisions with social norms and	

expectations that prevail among the users of a platform. These approaches naturally are not limited to enhancing the transparency of Terms and Policies as such. They may also be used as a tool to collect crowd-sourced suggestions for amendments and potential improvement by the platform provider, or even to create an agency for public discussions that criticize specific platform provisions."

On the whole, participatory transparency approach can help "to overcome the currently low level of user interest and can improve the users' awareness of the existence of a platform's Terms and Policies […]. The readability of legal texts is improved when the meaning of specific provisions is explained to a user […]. By doing that, the legal jargon can be translated into a text that the user actually understands […]."

"The platform providers, on the other hand, benefit from user participation by having an active, more satisfied user base, which for the either means a competitive advantage or, in monopolistic markets, increased legal certainty vis-à-vis judicial controls of general terms and conditions, or efforts in corporate social responsibility."

Even though the concept of participatory transparency "might enhance knowledge and understanding of Terms and Policies", one have to bear "in mind that both sides – users and platform providers – need incentives to participate" in this whole process. "Currently, both sides may find a lack of such incentives. A platform provider may decide not to endorse the outcome of a participatory transparency process for fear of losing control over the platform, thus risking his business model. […] A lack of incentive may also discourage users if there is no guarantee that their efforts will be noticed or appreciated by the provider."

Title Fine-Grained User Privacy from Avenance Tags	
published in Computing and Information Science Technical Reports. Department of Computer Science, Cornell University	
Year 2014	Authors Eleanor Birrell, Fred B. Schneider
Setting of the experiment "This paper suggests a new, practical, and expressive policy tag scheme that would enable users to express both control-based and secrecy-based restrictions. We identify key design goals, explore various design choices that impact these goals, and outline a proposed implementation called avenance tags that realizes these goals."	
Research question How would a new, practical and expressive policy tag scheme look like?	

Results *(copied from abstract/conclusions of the publication)* "Five goals-derived from the shortcomings identified in Section 2-motivate the design of our scheme. (1) Expressiveness: Users should be able to control how their data are used as well as what data become known (both by a service provider with which they interact and by third parties). (2) Scalability: The burden placed on users should be reasonable, even if users interact with many service providers. (3) Transparency: Privacy policies should be easily understood and transparent. They should clearly specify how observed data and derived values are used. (4) User Policy Revision: Users should be allowed to revise privacy policies and, thereafter, should enforce the revision. (5) Enforcement: Some enforcement mechanism ensures policy compliances. In order to realize these goals, we propose a scheme called avenance tags." "Avenance tags are a new proposal for enhancing Internet privacy. They implement a privacy policy language that combines control with secrecy to solve the problem of expressiveness, and they are deployed within the context of a system designed to address the other shortcomings of notice and consent. While the described avenance ecosystem is a long way from practical deployment, we believe it offers an interesting, viable avenue for future work. And we are now attempting a prototype implementation."

Title Are They Worth Reading? An In-Depth Analysis of Online Advertising Companies' Privacy Policies	
published in Non-reviewed DRAFT paper presented at the 42nd Research Conference on Communication, Information and Internet Policy (TPRC 2014)	
Year 2014	Authors Lorrie Faith Cranor, Candice Hoke, Pedro Giovanni Leon, Alyssa Au
Setting of the experiment In January 2014 the authors "retrieved a comprehensive list of tracking companies from Evidon's online database. This list had 2,750 companies under various non-mutually exclusive categories including, ad networks, ad servers, ad exchanges, analytics, optimizers, supply-side and demand-side platforms, data management platforms, publishers, among others. It also included theliations (if any) that these companies had	

with self-regulatory organizations." They "also obtained a list of the 36 largest tracking companies according to the 2013 Evidon global report."

They began their analysis "with three sets of 36 companies: The 36 largest companies; 36 member companies randomly selected from the set of companies that Evidon reported were aliated with either of the two largest self-regulatory organizations (Network Advertising Initiative and Digital Advertising Alliance) in January 2014; and 36 companies randomly selected from the set of non-member companies. During the initial analysis process the size of the sets changed. […] [The] final set was then comprised of 37 large, 33 member and 36 non-member companies."

They further decided to consider a company "as a member only if it appeared in the DAA or NAI web-sites and to compare practices of member and non-member companies as well as practices of large and random companies." Therefore, the authors "compared practices of companies in each of the following sets: large companies that were DAA or NAI members, hereafter referred as *large members*, non-large companies that were DAA or NAI members, hereafter referred as *random members*, large companies that were not members, hereafter referred as *large non-members*, and random companies that were non-members. hereafter referred as *random non-members*."

Finally, they "investigated 59 practices pertaining to collection, sharing, use, retention, user consent, access, contact, special provisions for children and European residents, security and user education."

Even though the authors attempted to analyze privacy polices from 106 online tracking companies as mentioned above, they "found that many non-member companies either did not have an online privacy policy, had a privacy policy that was not intended for tracked Internet users, or had websites written in a language other than English. Only 84 of the 106 companies [they] examined had a privacy policy written in English, and only 75 of those had a privacy policy that included relevant content for tracked users."

That is why they only "analyzed the privacy policies of 75 online tracking companies", "compared privacy policies from large companies, companies that are members of self-regulatory organizations, and non-member companies" and "evaluated these policies against self-regulatory guidelines".

Research question

"Assessing whether privacy policies contain information relevant to users to make privacy decisions"

Results

(copied from abstract/conclusions of the publication)

Even though information sharing is unsurprisingly common, "companies tend to conceal their sharing partners' usage of that information. Half of the evaluated companies do not specify their data retention period. Moreover, most companies do not provide options to stop data collection and less than a third provide opportunities to opt out of targeted ads

directly in their privacy policies. Most companies do not provide any access to collected information. Further, most companies are unclear or silent about collection and use of non-PII considered sensitive such as income range or health conditions. Large companies and ad industry self-regulatory association members exhibit relatively more comprehensive privacy policies." Furthermore, the "current state of online advertising self-regulation does not provide the level of transparency and control that users demand. In addition to unusable privacy policies, the combination of advertising companies functioning as third-parties (i.e., not user-facing), and the widespread sharing of information among tracking companies creates additional transparency challenges." Also the "lack of consistent terminology to refer to aliate and non-aliate partners, and the mix of practices for first-party and third-party contexts make it challenging for users to clearly assess the risks and make meaningful decisions."

The authors "found that most of these companies are silent with regard to important consumer-relevant practices including the collection and use of sensitive information and linkage of tracking data with personally-identiable information. Policies lacked a clear and consistent definition of non-aliates with whom online tracking companies share user information. Policies also mixed practices that apply to information collected in first- and third-party context, and they are rarely intended only for tracked users, but more often intended for different audiences simultaneously (e.g., partners, website visitors, and tracked users). These facts would make it very dicult and sometimes impossible for users to determine what practices apply to them and be able to properly assess the associated privacy risks. Unless these problems are fixed, ongoing efforts to use natural language processing (NLP) techniques and crowd sourcing to interpret privacy policies will not be able to improve transparency and empower users to protect their privacy in the context of OBA. We also evaluated these policies against self-regulatory guidelines and found that many policies are not fully compliant. Furthermore, while member companies are more likely to offer the opportunity to opt out of targeted ads, previous research has shown that users are concerned about online tracking and interested in controlling data collection, an option that companies are not offering. We have provided recommendations to improve clarity and usability of online tracking companies' privacy policies."

Title	
Knowledge-based Individualized Privacy Plans (KIPPs): A Potential Tool to Improve the Effectiveness of Privacy Notices	
published in	
Workshop on the Future of Privacy Notice and Choice, Carnegie Mellon University June 27, 2014	
Year	Authors
2014	Masooda Bashir, Kevin A. Hoff, Carol M. Hayes, and Jay P. Kesan

Setting of the experiment Used a „two-part online survey centered around consumer knowledge and opinions. The survey link was distributed primarily through email at the University of Illinois at Urbana-Champaign. We collected about 500 responses for each part of the survey, with the majority of responses coming from individuals between the ages of 18 and 25. [...] In addition to the opinions, we also conducted an extensive evaluation of online privacy knowledge.”
Research question Are KIPPs a potential tool to improve the effectiveness of privacy notices?
Results *(copied from abstract/conclusions of the publication)* “Only 43% of respondents indicated that they had ever refused to use a website strictly because of the website’s privacy policy or terms of service agreement. This provides further evidence that privacy notices do not usually influence consumer behavior.” “Thus, by addressing certain crucial gaps in preexisting knowledge, KIPPs could promote increased readership rates and subsequently enhance the role of privacy notices in informing consumer decision-making.” “Deficiencies in consumer knowledge must be addressed in order to improve the effectiveness of the existing “notice and choice” approach to digital privacy. Privacy notices could likely play a greater role in informing consumer decision making if they better accommodated the needs of diverse individuals with varying degrees of background knowledge. In this paper, we have proposed a new instrumentality, the Knowledge-based Individualized Privacy Plan (KIPP), which would aim to improve consumer comprehension of the significance of privacy notices by personalizing information based on different levels of preexisting knowledge. We are enthusiastic about the potential contributions that KIPPs could make as a tool to improve the effectiveness of notices within the “notice and choice” approach to digital privacy. In order to be useful in an ever-changing online environment, KIPPs will need to address the needs of consumers, businesses, and relevant third parties. Thus, future research is needed to examine the practicality, usability, and design of KIPPs, as well as potential ways to increase consumer demand for more comprehensible privacy notices. In addition, more research is needed to assess what consumers from across the world currently understand about digital privacy and related issues. Performing this type of research will be crucial in order to guide future efforts, such as those related to KIPPs, aimed at increasing consumer privacy knowledge and promoting informed consumer decision-making.”

Title A Field Trial of Privacy Nudges for Facebook	
published in CHI 2014 , Apr 26 – May 01 2014, Toronto, ON, Canada, ACM 978-1-4503-2473-1/14/04	
Year 2014	Authors Yang Wang, Pedro Giovanni Leon, Alessandro Acquisti, Lorrie Faith Cranor, Alain Forget, and Norman Sadeh
Setting of the experiment “Our work makes two contributions. First, we developed an experimental platform that modifies Facebook’s interface and collects users’ behavioral data to operationalize and evaluate the concept of Facebook privacy nudges. Second, we identified key aspects worth considering when designing and evaluating a privacy nudging system.” „Our study focused on two types of nudges: one that reminds users about the audience for their post, and one that encourages users to pause and think before posting.” In the first type, users see profile pictures and information about the people, who will see the post, the second type “introduced a visual delay of 20 seconds after a user clicked the “post” button before publishing the submitted post. During the countdown, the user could cancel this post.” After the first pilot, the delay was reduced to 10 seconds and three links were added: “post now”, “edit”, and “cancel”. The study was tested in a 6-week field trial with 28 Facebook users during April and May, 2013. Participants had to satisfy these criteria: “active adult US Facebook users who posted or commented at least once per day on average; native English speakers who posted in English and used Chrome, primarily, to access Facebook.” In the first three weeks they collected data without nudging interventions and ended with a mid-term survey, in the last three weeks, in addition to data collection they also introduced the nudges and a final survey at the end of the six weeks.”	
Research question “In this paper, we describe the design and evaluation of mechanisms that nudge Facebook users to consider more carefully the content and context of their online disclosures through visual cues and time delays.”	
Results *(copied from abstract/conclusions of the publication)* “To help individuals avoid such regrets, we designed two modifications to the Facebook web interface that nudge users to consider the content and audience of their online disclosures more carefully. We implemented and evaluated these two nudges in a 6-week field trial with 28 Facebook users. We analyzed participants’ interactions with the nudges, the content of their posts, and opinions collected through surveys. We found that reminders about the audience of posts can prevent unintended disclosures without	

major burden; however, introducing a time delay before publishing users' posts can be perceived as both beneficial and annoying. On balance, some participants found the nudges helpful while others found them unnecessary or overly intrusive. We discuss implications and challenges for designing and evaluating systems to assist users with online disclosures." "While the field study we presented in this paper should be considered exploratory, our results suggest that privacy nudges have the potential to be a powerful mechanism to assist users in avoiding unintended disclosures."

Title The Use of Privacy Icons and Standard Contract Terms for Generating Consumer Trust and Confidence in Digital Services	
published in CREATe Working Paper 2014/15	
Year 2015	Authors Lilian Edwards, Wiebke Abel
Setting of the experiment Examination of "two possible paths for UK industry to re-establish consumer trust and confidence in the cloud, and in consumer digital services in general." First, the authors consider the "use of icons and labelling as a means to more effectively communicate complex and lengthy privacy policies to consumers." Secondly, they assess "the use of standardised contract terms or templates in relevant business-to consumer (B2C) [...]."	
Research question Might icons and labelling as well as standardised contract terms or templates be helpful to re-establish consumer trust and confidence?	
Results *(copied from abstract/conclusions of the publication)* The authors conclude that empirical research assessing the success of both icons and labels is extremely limited, but it seems that end-users understanding of privacy policies can be improved by such initiatives. However, privacy icons "merely highlight key points and are not meant to be complete. This raises the issue […] that the picture a user gains from the "icon" privacy policy may be very different from the one given by the entire written, legal policy – and of possible consumer complaints and legal disputes." This phenomenon is described "as the 'bad icon' problem". Another "problem with icon or label schemes will be their international scope. Consumers buy digital products and services globally not locally; while an icon /labelling system might be developed only for	

use by UK service providers and aimed at UK consumers only, its usefulness might then be limited to industry sectors strongly tied to national borders (e.g. energy suppliers). Given differences in privacy laws, especially between the EU and the US, but also between the UK and many other EU states, and the disparity of laws throughout Asia, a system that tried to label compliance, or even "factual" privacy features, might be very difficult to build on an international scale."

In this authors' opinion, standard contracts can also "be an effective means to ensure that consumers are sufficiently protected against industry standard terms or service level agreements that are unfair and/or significantly weighted in favour of the provider. In this domain, standard contracts can be seen as 'regulated privacy policies'." Compared with icons, which "merely gives consumers greater or clearer notice" or more control, regulating privacy policies "can provide minimum guarantees of privacy protection and can therefore engender greater trust from consumers in the market. Ideally regulated privacy policies would also be represented by clear multi-layered notices which might combine full legal details, plain English short notices and iconic representations."

Title A Psychological Account of Consent to Fine Print	
published in Institute for Law and Economics at the University of Pennsylvania, Research Paper No. 14-22	
Year 2014	Authors Tess Wilkinson-Ryan

Setting of the experiment

The Essay uses five different studies to find an answer to the research question.

"The Essay proceeds as follows. In Part I, I set up the problem with descriptive, legal, and theoretical perspectives on consent to fine print in consumer contracting. Part II lays out evidence, from existing and new research, that consumer contracting invokes conflicting norms. Study 1 in this Part tests the relationship between contract procedures and inferences of consent, and the results show evidence that subjects may believe that it is unreasonable to expect consumers to read terms in some forms, but that they would nonetheless hold those non-reading consumers accountable for transactional harms that occur ex post. Parts III and IV make the case that there are psychological explanations—involving a particular set of motivations, intuitions, and cognitive processes—for these differential evaluations of consent at the formation and enforcement stages of contracting. In Part III, I present Studies 2 and 3, offering evidence that the mere fact of consumer harm motivates inferences of consumer consent to that harm. Part IV includes Studies 4 and 5, which show that consumer decision-making is a highly salient link in the chain of causation that explains a

transactional harm. Part V concludes with a discussion of these findings in light of procedural justice research, and I argue that the next step in the moral psychology of contracting is the development of a robust body of research on procedural justice in the consumer marketplace.”
Research question How do ordinary consumers understand their contractual obligations when formation of most contracts is perfunctory, but the moral and legal rhetoric of contract enforcement is robust? How seriously should contract law take consent in a world in which consumers must consent lightly to most of their contractual obligations?
Results *(copied from abstract/conclusions of the publication)* “This Essay aims to unpack the beliefs, preferences, assumptions, and biases that constitute our assessments of assent to boilerplate. Research suggests that misgivings about procedural defects in consumer contracting weigh heavily on judgments of contract formation, but play almost no role in judgments of blame for transactional harms. Using experimental methods from the psychology of judgment and decision-making, I test the psychological explanations for this disjunction, including motivated reasoning and reliance on availability heuristics. Many commentators have argued that even though it is true that disclosures are probably ineffective, they “can’t hurt.” I conclude with a challenge to that proposition — I argue that the can’t-hurt attitude may lead to overuse of disclosures that do not affect consumer decision-making, but have implicit effects on the moral calculus of transactional harms.”

Title Behavioural Sciences and the Regulation of Privacy on the Internet Nudging and the Law - What can EU Law learn from Behavioural Sciences?	
published in Sibony A-L, . Alemanno, A., eds. (forthcoming). A working paper on this topic has been presented at the 6th Annual Privacy Law Scholars Conference (Berkeley, 7 June 2013), and the Nudging in Europe conference (Liège, 12-13 December 2013)	
Year 2014	Authors Frederik Zuiderveen Borgesius
Setting of the experiment The author describes practices of behavioural targeting and related privacy problems and discussed the current regulatory regime. He analyses the problems with informed consent through the lens of behavioural sciences and information asymmetry, transaction costs and biases that influence people’s privacy decisions. At the end he	

discusses two ways to improve privacy protection.
Research question How could we improve privacy protection?
Results *(copied from abstract/conclusions of the publication)* The author argues for a combined approach of protecting and empowering people. Data protection rules should be tightened, and should be enforced more strictly. He argues that policymakers could also try to nudge Internet users towards disclosing less data.

Title Automated Experiments on Ad Privacy Settings: A Tale of Opacity, Choice, and Discrimination	
published in Proceedings of Privacy Enhancing Technologies Symposium, July 2014	
Year 2014	Authors *Amit Datta, Michael Carl Tschantz, Anupam Datta*
Setting of the experiment The authors ran “experiments where automated agents simulating users interact with Google and content providers”. After that they measured ”how these interactions alter the ads and settings that Google shows.” “The experimenter randomly partitions the agents to a control group and an experimental group […]. To each group, the experimenter applies the group’s respective treatment by having the agents perform actions producing inputs to Google. Next, the experimenter takes measurements of the outputs Google sends to the agents, such as ads.” They “could only run ten agents in parallel given [their] hardware and network connection. Agents running at different times are not exchangeable since Google can determine the time at which an agent interacts with it.” AdFischer “automates the simulation of having a particular interest or attribute by visiting webpages associated with that interest or by altering the ad settings provided by Google. It automates the collection of ads shown to the simulated users and the settings that Google provides. It automatically analyzes the data to determine whether statistically significant differences between groups of agents exist. To do so, AdFisher uses machine learning to automatically detect differences and then executes a test of significance specialized for the difference it might have found.” Using AdFisher, they “conducted 20 experiments using 16,570 agents and that collected 570,000 ads.” Some of these experiments are briefly described in the result section.	

Research question Presentation of AdFischer, an automated tool that explores how user behaviors, Googles ad, and Ad Settings interact
Results *(copied from abstract/conclusions of the publication)* Discrimination: They used "AdFisher's ability to automatically select a test statistic to check for possible differences to test the null hypothesis that the two experimental groups have no differences in the ads they received." Therefore, the authors "set the gender of one group to female and the other to male. In one of the experiments, the agents went straight to collecting ads; in the others, they simulated an interest in jobs." They "found that females received fewer instances of an ad encouraging the taking of high paying jobs than males." Transparency: "AdFisher tests the null hypothesis that two groups of agents with the same ad settings receives ads from the same distribution despite being subjected to different experimental treatments. Rejecting the null hypothesis implies that some difference exists in the ads that is not documented by the ad settings." They "ran a series of experiments to examine how much transparency Google's Ad Settings provided" and "checked whether visiting webpages associated with some interest could cause a change in the ads shown that is not reflected in the settings." The authors "ran such experiments for five interests: substance abuse, disabilities, infertility, mental disorders, and "adult" websites." They found "that settings did not change at all for substance abuse and changed in an unexpected manner for disabilities." Choice: They "tested whether making changes to Ad Settings has an effect on the ads seen, thereby giving the users a degree of choice over the ads. In particular, AdFisher tests the null hypothesis that changing some ad setting has no effect on the ads." Therefore they "tested whether opting out of tracking actually had an effect by comparing the ads shown to agents that opted out after visiting car-related websites to ads from those that did not opt out." They "found a statistically significant difference." They also tested "whether removing interests from the settings page actually had an effect. To do so, [they] set AdFisher to have both groups of agents simulate some interest. AdFisher then had the agents in one of the groups remove interests from Google's Ad Settings related to the induced interest. [They] found statistically significant differences between the ads both groups collected from the Times of India for two induced interests: online dating and weight loss." Conclusion: The authors "found the presence of discrimination, opacity, and choice in targeted ads of Google. […] Ideally, tools, such as Ad Settings, would provide a complete

representation of the profile kept on a person, or at least the portion of the profile that is used to select ads shown to the person. Two people with identical profiles might continue to receive different ads due to other factors affecting the choice of ads such as A/B testing or the time of day. However, systematic differences between ads shown at the same time and in the same context, such as those we found, would not exist for such pairs of people. Lastly, [they] found that Google Ad Settings does provide the user with a degree of choice about the ads shown. In this aspect, the transparency tool operated as [they] expected. In at least some cases, removing interests from the settings behaved in a manner consistent with expectations and removed ads related to the removed interests."

Title The No Reading Problem in Consumer Contract Law	
published in Stanford Law Review 2014: 545-600. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2341840	
Year 2014	Authors Ian Ayres, Alan Schwartz

Setting of the experiment

<u>Theoretical Framework</u>

How does a market behaves when the no-reading problem exists? "Seller maximize profits but only a subset of consumers has correct expectations". Because the authors focus mainly on disclosure, they "abstract from competition issues to model a market with one seller. "

First of all, they assume that "all consumers have correct expectations […] and show that the seller nevertheless may offer an inefficient contract. […] The seller is facing a population of informed consumers who differ in the utility they derive from contract terms. […] The seller focuses on the preferences of the marginal consumer because, if he mistakes those, marginal consumers may exit the market." Then they assume that "the seller is considering whether to increase contract quality. […] The question the seller thus asks is whether the marginal consumers' willingness to pay for a better quality contract would increase by as much as or more than the seller's increased cost. […] when the sensitivity of average consumers to increases in contract quality exceeds the sensitivity of marginal consumers, contracts will exhibit inefficiently low quality even when demand is 'correct': that is, when consumers have correct expectations. The average consumer would be willing to bear the cost of an increase in contract quality but the seller will not make that increase."

The authors then relax "the assumption that demand is correct, and […] show that markets are flawed more by optimism than by pessimism. […] those pessimist who are

in the market have an artificially low willingness to pay. […] the seller has an incentive to cure pessimistic mistakes. It is otherwise with optimists. These consumers are either incorrectly in the market or are in but are willing to pay too much for what they get. The seller has no incentive to inform optimists."

A Preliminary Term-Substantiation Study of the Facebook EULA

"From late November 2012 through early January 2013, [the authors] administered a survey designed to illustrate the type of research a mass consumer company could undertake […]." They "set up a table at four different public settings and offered subjects $5 to take a fifteen-minute Yale Law School survey. The survey asked a series of twenty-five questions concerning specific terms included in Facebook's Statement of Rights and Responsibilities, and how important those terms were to the respondent." The authors "also asked the respondents a number of ancillary questions about the basis of their knowledge (e.g., whether they use Facebook and whether they had previously read Facebook's terms of use) and the respondent's socio-demographic identity (e.g., respondent's age, gender, race, and income). A total of 242 respondents completed the survey. One-hundred forty-three of our respondents were Yale-affiliated and participated by answering the survey at campus locations. Ninety-nine of [the] respondents (who were, for the most part, not affiliated with Yale) participated by answering the survey at an off-campus New Haven location (just inside the entrance of a grocery store). The vast majority (85%) of respondents were Facebook users and reported not having previously read Facebook's Statement of Rights and Responsibilities (77%). Broadly speaking, the demographics of the survey population were representative of Facebook's user base in the United States. [The] population was quite young – somewhat younger, in fact, than Facebook's users, with approximately 75% between the ages of 18 and 34.This compares to approximately 50% of Facebook's user base in the U.S. The sample was slightly more female than male (52% female, 45% male, compared to Facebook's breakdown of 55% female, 45% male in the United States)." They "achieved significant racial diversity in our survey population […]. Respondents were wealthier than the average American[…]. Finally, because one of […] four survey locations was in the Yale Law School, a significant portion of our population (29%) had some law school education."

The "twenty-five core questions about Facebook terms concerned several of the different sections of the Statement of Rights and Responsibilities, including Privacy and Advertising, Safety, Registration and Account Security, Protecting Other Peoples' Rights, Mobile & Other Devices, Ammendments and Disputes."

The "survey design also included two dimensions of randomization. First, [the authors] randomized the order of the questions – assigning respondents at random to 'forward' and 'backward' conditions -- which differed only in that the backward condition reversed the order of all the questions (such that the first question became the last and vice versa). […] Second, and more centrally, [they] randomly assigned subjects to either a group that added an 'I have no idea' answer to each of the twenty-five questions or to a group that excluded this option. Thus, respondents in the 'no idea' group were given the option of answering each question by indicating that they had no idea while the 'best

guess' group was given choices that excluded this 'no idea' option. Randomizing on this second dimension allows [them] to test the impact of 'forcing' subjects to express an opinion when they may have little confidence in their knowledge about the content of particular terms."
Research question The authors "argues that consumer protection law should focus on 'term optimism' – situations in which consumers expect more favorable terms than they actually receive." They "propose a system under which mass market sellers are required periodically to engage in a process of 'term substantiation' through which sellers would learn whether their consumers held accurate beliefs about the terms of their agreement."
Results *(copied from abstract/conclusions of the publication)* <u>Theoretical Framework</u> "The model yields three results. First, the principal policy concern is optimism: contracts fall in quality as consumers become more optimistic about their content. Optimistic consumers are willing to pay too much for bad contracts so the seller has too little incentive to offer good contracts. Second, uniformed consumers who are 'in' the market are relevantly alike: that is, all of them would benefit from disclosure of the dame unexpectedly disadvantageous terms. As a consequence, a term substantiation study that focuses on actual or potential buyers would have external validity. In the model [..], consumers with minority preferences over contract terms are not in the market at all. Third, having several sellers has an additional virtue: the market may serve consumers with minority preferences." "[…] the seller, as a general matter, will degrade contract quality even when he faces correct demand. Relevant here, term optimism exacerbates the problem. Because optimists have an artificially high willingness to pay, their presence widens the gap between the average and marginal consumers. Put another way, optimists punish the seller less than informed consumers for degrading contract quality because the optimists are willing to pay too much for whatever contract the seller offers. Hence, the more optimists there are in a market the worse market contracts are for everyone. " The authors conclude that "disclosure should focus on reducing term optimism." They "propose a system under which mass market sellers are required periodically to engage in a process of 'term substantiation' through which sellers would learn whether their consumers held accurate beliefs about the terms of their agreement." The seller should also "provide warnings about such terms in a cautionary standardized box." <u>A Preliminary Term-Substantiation Study of the Facebook EULA</u> The authors "find that 41% of the 'no idea' responses would have been accurate responses if the respondents had not been given this option. This percentage is statistically smaller than the 51% accuracy of the respondents who were given the 'no idea' option but choose nonetheless to express an opinion." Thus, the authors "infer that

the people who answer ‘no idea’ were less knowledgeable than those who volunteered to express an opinion. But their inferred accuracy of 41% was still statistically better than random guessing.”

Furthermore, their survey “found systematic consumer optimism with regard to some terms […]. A statistically significant majority of respondents in the ‘best guess’ treatment group optimistically believed that four terms were more favorable to them than the actual terms.” In the authors’ point of view, “these terms would need to be included in a standardized warning boy in decreasing order of importance to consumers.”

They first tested the impact of the two randomized treatments. As expected, they “see no significant difference in the warnability from the ‘backward’ treatment groups relative to the omitted ‘forward’ treatment group. Also as expected, we find the respondents in the ‘no idea’ group had a statistically significant increased chance of giving a warnable answer […].”

“The specifications next estimate the impact of aspects of the respondent‘s relationship to the Facebook website. The regressions suggest that respondents were less likely to give warnable answers if the respondents reported having at an earlier time read the Facebook contractual terms.” They “also find […] that respondents were less likely give an inaccurate optimistic or ‘No idea’ response with regard to terms that they assessed as being important. But somewhat counterintuitively, the regressions estimated that registered Facebook users were more likely than non-Facebook users to give warnable answers (although this effect was not statistically significant in the second specification).

The second specification added a variety of controls related to the type of the respondent (including a number of demographic controls). There was no statistical difference in the likelihood of giving a warnable answer for Yale versus non-Yale respondents, but (as might be expected) respondents with some legal training were statistically less likely to give a warnable answer. [The authors] found no statistical difference in gender, but found that African American and American Indian respondents were statistically more likely to give warnable answers. The specification also found that respondents reporting income over $350,000 were statistically more likely to give warnable answers (than the omitted category or respondents with reporting annual household incomes of $60,000 to $99,999).”

Title A Generalization of Advertising Avoidance Model on Social Network	
published in Working Paper in Review. http://dee.uib.cat/digitalAssets/313/313123_Rejon1.pdf	
Year 2014	Authors Rejón-Guardia, F.; Sánchez-Fernández, J.; and Muñoz-Leiva, F.

Setting of the experiment

"The subjects interviewed for this study were all users of ISNs [Internet Social Networks]. The subjects were required to have previous experience on the Internet; a variable that was taken into account to determine the validity of the data. In order to simulate a Web surfing context, [the authors] developed a closed online environment that was housed in the server of the Department of Marketing and Market Research at the university to which the authors of this study belong. This surfing environment permitted the subjects to surf and view the three social networks", Myspace, Facebook and Tuenti. "This simulated environment included the most widely-used Web advertising formats in which variety of ad messages were placed using real information and products […]."

"[...] the final number of valid questionnaires was 262."

"To measure intrusiveness and irritation, [the authors] used the scale proposed by Edwards et al. (2002) with 7 and 5 questions […]. The first scale asked subjects about their perceptions on the advertisements to which they were exposed. The irritation scale included a series of adjectives related to irritation caused by advertising. The ad clutter and cognitive avoidance scales were adapted to our particular study from the works by Cho & Cheon (2004) and Li & Meeds (2007) and included 3 and 8 items […]. The ad clutter scale included items to measure over advertising, ad irritation and the perception that the Internet is exclusively an advertising vehicle. This construct encompasses intrusiveness (reactance), competitiveness (interference) and load (overload). Finally, the cognitive ad avoidance scale included questions regarding the different attributes and reactions of users toward ISN advertising. All of the scales were 7-point Likert scales. […] Ad effectiveness was measured through memory of the advertising message appearing on the ISNs by means of a dichotomous scale."

Research question

Provision of "a framework for the field of online information that specifically focuses on the effectiveness of online ads through an analysis of the main determinants of effectiveness, concretely, clutter, intrusiveness, irritation and avoidance."

Research questions:

1. "There is a direct and positive relationship between ad clutter and cognitive avoidance."
2. "There is a direct and positive relationship between intrusiveness and cognitive avoidance."
3. "There is a direct and positive relationship between irritation and cognitive avoidance."
4. "There is a direct and negative relationship between cognitive avoidance and brand recall (ad effectiveness)."
5. "There is a second-order latent construct called advertising offensiveness formed by the direct and positive relationship of the ad clutter dimension."

6. “There is a second-order latent construct called advertising offensiveness formed by the direct and positive relationship of the perceived intrusiveness dimension.”
7. “There is a second-order latent construct called advertising offensiveness formed by the direct and positive relationship of the perceived irritation dimension.”
8. “There is a direct and positive relationship between advertising offensiveness and cognitive avoidance.”

Results

“Research questions, RQ5, RQ6, and RQ7 were not rejected following the data analysis […]. This suggests that the variables of perceived ad clutter, intrusiveness and ad irritation comprise a second-order construct called advertising offensiveness. This construct shows the degree to which negative factors are manifested when ISN users view advertising. Finally, a direct and positive relationship was found to exist between advertising offensiveness and cognitive avoidance (RQ8). Hence, when ISN users perceive factors they consider undesirable which in turn lead to the sensation of perceived clutter, ad intrusiveness or irritation with ads, there will be a high degree of ad avoidance in the medium. In contrast, we can only accept the partially significant relationships provided by hypothesis RQ4 given that advertising effectiveness in terms of ad memory was only found to be significant for the Tuenti and quasi-significant differences were found when comparing Tuenti to MySpace […]. Likewise, a slightly less direct and positive relationship was found for the Tuenti between the three dimensions and the second-order construct. This could be due to the fact that the messages appearing on Tuenti are simpler and clearer in form and therefore causeless negative attitudes than the advertising messages in the other ISNs. Moreover, the multi-group analysis does not show statistically significant differences between the different ISNs in terms of how the relationships behave.”

Title	
Do Consumers Read Terms of Service Agreements When Installing Software? A Two-Study Empirical Analysis	
published in	
International Journal of Business and Social Research 4(6): 137-145.	
Year	Authors
2014	Maronick, T. J.
Setting of the experiment	
This paper answers the research questions on the basis of two surveys.	
Study 1.	

"The first study was an on-line survey of 151 consumers age 21 or older who had installed software on their home computer in the prior two months. The sample was drawn from an on-line panel of individuals who have agreed to participate in surveys on a periodic basis. Respondents were first screened to determine that they install software on their home computers and how frequently. They were then asked the likelihood that software they were installing would infect or compromise other software on their computer and, if the software did infect/compromise other software, who would be responsible for the damage, i.e., the software company or themselves. They were then asked how much of the agreement they generally read, and reasons they don't read any or more of the agreements. Respondents who could recall seeing a 'Terms of Service' or 'Terms of Use' agreement screen/window on the last software they had installed on their home computers (n=101) were asked what options were available to them with the TOS screen/window and which option they selected. They were then asked how long, in seconds and/or minutes they spent reading the TOS agreement and reasons why they didn't read any or more of the agreement when installing their last software on their computer." Study 2 "In order to assess consumers' actual experiences installing software, Study 2 was a simulation whereby consumers 'installed' software from the internet in a mall-intercept environment. The research protocol captured their behavior, expectations, and perceptions as they installed and after they installed the software. A sample of 160 individuals who are in the target market for business-communications software were surveyed in shopping malls in four geographically diverse US locations. Prospective respondents who had been qualified in the mall were asked to assume they were installing the software on their home computer from the internet and were asked to go through the process of installing it on the computer before them. The software employed in Study 2 was a totally new product from a new company. Thus, there is no likelihood of prior experience with either the company or its software affecting the outcomes observed during the simulation. Once the respondent began the installation process, the researcher observed and recorded the amount of time the respondent spent at selected set-up screens, including the 'Terms of Service Agreement' screens, and recorded the action taken by the respondent at the selected screens."
Research question The research questions are: "1) how often do consumers say they read any or all of the TOS agreement by scrolling through the numerous pages, 2) how much time do they say they spend reading the TOS agreements, 3) is there any relationship between the time spent reading the TOS agreement and the perceived risk of damage […] to their computer or other software on their computer from the software they are downloading and 4) is there is any relationship between the length of time consumers say they spend reading TOS agreements and the amount of time they actually spend reading them?"
Results Hypothesis:

1. "The majority of consumers read less than half of TOS Agreements":
   The results of Study 1 show […] that 45% of respondents claim to read 'less than half' of the TOS agreement and there is no significant difference between the percent saying they read 'more than half' of the agreement (37.9%) and those who say they read 'very little' or 'none' of the TOS agreements (41.1%). Therefore, based on respondents claimed time spent reading the TOS agreement, Hypothesis 1 must be rejected. However, if one accepts the fact that the average Terms of Service agreement is 6,656 words long and written at a 12th grade level or higher, that the average reading rate for American adults is 250 to 300 words per minute […] and the fact that 61% of respondents spent 30 seconds or less reading the TOS agreement when installing their last software […], then one must conclude that consumers do not read very much of the Terms of Service agreements and accept Hypothesis 1."
2. "Amount of time spent reading contract is directly proportional to perceived risk of damage to other software on computer":
   "[…] 27% of respondents in Study 1 indicated there was some chance (i.e., likely or very likely) the software they recently installed could have infected or compromised other software on their computer, whereas 21% it was not at all likely or unlikely that the software would damage other software. On the other hand, a significantly […] lower percent […] said there was a risk (i.e., likely or very likely) when installing the software in the simulation in Study 2. This difference more than likely reflects familiarity with the particular, well-known software used in the simulation. However, there is no significant difference in the amount of the TOS agreement read and the perceived likelihood of damage to the computer or other software. Also, there is no significant difference in the time spent reading the TOS agreement when installing the last software or when installing the software in the simulation and the perceived likelihood of damage to other software on the computer. Therefore, Hypothesis 2 that the amount of time reading TOS agreements is proportional to the perceived risk of the software to other software on the computer is not accepted."
3. "The actual amount of time actually spent reading TOS is inconsistent with claimed amount of TOS agreement generally read":
   "A comparison of the claimed amount of TOS agreements respondents generally read […] and the amount of time respondents claim to spend reading the TOS agreement on their most recent software installation […] in Study 1 shows significant variances. […] Therefore, one can only conclude that the time spent […] is not consistent with the amount of the TOS respondents claim to read. These conclusions are confirmed with Study 2 where 58.7% of respondents in the software installation simulation clicked the 'Agree' option (i.e., without reading any of the TOS) and 27.2% of those who clicked 'Next' to read the TOS spent less than 30 seconds reading the 6,000 word agreement. As a result, a total of 75.6% of respondents in the simulation spent less than one minute reading the TOS. Therefore, Hypothesis 3 is accepted."
4. "Primary reasons for not reading TOS agreements are length of contract and

formatting factors such as density of agreement, type/font size, and terms/legalese": "[…] respondents' comments respondents during the software installation simulation (Study 2) confirm the Study 1 findings. […] 63% of respondents said the reason they didn't read the TOS, or read very little of it, was because it was 'boring, tedious, too long, or too wordy'. […] Therefore, Hypothesis 4 is supported as to length of contract as a reason for not reading, but not supported as to other formatting factors of the agreement […]."

Title	
How Effective is Mandatory Disclosure?	
published in Columbia University. Working paper.	
Year 2014	Authors Mitts, J.

Setting of the experiment

Stage 1

"Stage 1 of this study seeks to identify terms in consumer contracts that are unexpected, as limiting disclosure to these terms is likely to be most efficient." Mitts "identify unexpected terms by surveying consumers as to whether they expect that a standard form contract contains a particular term. […] the stage 1 survey is composed of both actual and fictitious terms. This results in four categories of terms:

- Category 1: actual terms, unexpected
- Category 2: actual terms, expected
- Category 3: fictitious terms, unexpected
- Category 4: fictitious terms, expected"

The author "conducted the survey across two types of contracts: cell phone and credit cards."

Stage 2

"The purpose of stage 2 is to estimate the effect of mandatory disclosure on consumers' contracting decisions and understanding of contract terms. Stage 2 consists of an experimental design with three steps. First, eligibility is verified using [a] dynamic demographic filter […]. Second, participants are randomly assigned to five treatment groups on two dimensions—number of warnings and price discount—and asked to choose between two service providers that are otherwise identical except for the treatment. Finally, participants are quizzed regarding the content of the unexpected terms and asked two follow-up questions."

Research question
How “much disclosure maximizes consumer understanding while minimizing market distortions?”
Results
“This study has shown that warnings-based disclosure at the time of contracting may be effective, but only up to a point: too many warnings may drive consumers away from warned-of firms without leading to greater understanding in return. A long list of warnings may have a psychological effect that leads consumers to strongly prefer competitors, likely in an inefficient way. Moreover, greater discounts were unable to overcome this psychological effect, which suggests that the additional disclosure may impose an especially onerous burden on firms offering contracts containing a large number of unexpected terms. From a normative standpoint, this burden might be justified if it led to greater understanding of the unexpected terms on the part of consumers who saw many warnings. But the post-choice quiz indicates that after a certain point having more warnings does not necessarily yield greater virtually indistinguishable from those who saw three warnings. The additional disclosure has value—indeed, both treatment groups did better than the control group that was exposed only to one warning. But the absence of a major difference in consumer understanding between three and six warnings suggests that more is not always better. These results are consistent with the critique of Truth-in-Lending and similar disclosure regimes that an excess quantity of disclosure induces cognitive overload. This design can be critiqued as reflecting ‘contracting’ decisions that do not involve binding legal commitments or real money. […] This study’s results are consistent with at least two suggestions for improving mandatory disclosure regimes. First, a warning system at the time of contracting may not be the best way to accomplish the goal of ensuring that consumers receive adequate information regarding unexpected, unfavorable terms. Large-scale public education efforts by government regulators and consumer advocacy organizations may be a more effective way to inform consumers of terms that are unexpected in mass-market contracts. Limitations on consumer comprehension when information is presented in a warning box may not hold in other settings, i.e., news or social media. Warnings-based disclosure may therefore be much needed, but more successfully provided in a different forum. Another suggestion is to limit mandatory disclosure at the time of contracting to a small number of ‘highly unexpected’ terms. Regulators may simply conclude that because the costs of excessive warnings outweigh the benefits, mandatory disclosure at the time of contracting should contribute to an overall consumer protection regime by warning of the top three unexpected terms, for example. The burden of these warnings on service providers would be minimal, and even a small number may improve consumer understanding over simply expecting individuals to read the fulltext agreement. Some increase in information is better than none, particularly if it can be obtained with little harm to otherwise mutually beneficial transactions. Nonetheless, these suggestions should not detract from a central conclusion of this study: the additional disclosure did improve consumer understanding of the contract terms by 9-10%.”

Title	
Awareness of Behavioral Tracking and Information Privacy Concern in Facebook and Google	
published in Symposium on Usable Privacy and Security (SOUPS) 2014, July 9–11,2014, Menlo Park, CA.	
Year 2014	Authors Rader, E.

Setting of the experiment

Rader conducted "a 2 (Site: Facebook or Google Search) x 3 (Behavior: Link, Autocomplete or Ad) x 2 Sensitivity (High or Low) between-subject online experiment hosted by Qualtrics, in May 2013. Participants viewed a hypothetical situation that varied according to these three dimensions […]."

"The online experiment stared by displaying a hypothetical situation that varied by condition, designed to closely resemble common experience while using the web. […] Each condition was accompanied by a partial screen capture to illustrate what was happening, and the manipulation of Site and Sensitivity took place via the screen captures. […] Participants were asked a closed-ended and an open –ended privacy concern question, immediately after viewing the hypothetical situation:

1. Would you be concerned about unwanted access to private information about you in this scenario? [Yes, Maybe, No]
2. Please explain your answer to the previous question. [open-ended]"

After the privacy concern question, participants responded to a 16-item question that asked them to estimate the likelihood that Facebook or Google could collect different kinds of data about them […]. The motivation for asking about these items was to identify what kinds of 'tracking' users think may be going on when they use the web, and through later regression analysis to identify associations between these beliefs and the likelihood of privacy concern."

Research question

Investigation of "(1)whether users are concerned about privacy when they engage in common behaviors on the web that can enable automated disclosures to take place; (2) whether people are aware of different types of data that can be automatically collected about them when they use Facebook and Google Search; and (3) how the perceived likelihood of automated data collection might be related to privacy concern."

Results

"As expected […], more people answered No (377 participants) and Maybe (173 participants) than Yes (151 participants) when asked if they were concerned about unwanted access to private information."

Furthermore, “the results of this study reflect the general trend that participants who were asked about Facebook were more likely to report concern about unwanted access than participants asked about Google. After controlling for participants’ level of Internet Literacy and Privacy Preferences, participants were most likely to express concern in the Facebook: Ad conditions, while participants in the Google: Link: Low Sensitivity condition were the least likely group to express concern in the entire study. There is also some evidence in participants’ explanations to suggest that they believed clicking a link in Facebook discloses information about them, but that if the same action is part of a Google Search it is not a disclosure. […] Ads in Facebook were more a source of concern for participants than ads in Google, because they perceived that Google ads were associated with search queries (that participants just wouldn’t enter if they were sensitive), while Facebook ads were associated with personal characteristics (that participants might not want to reveal). Ads on Facebook contain evidence of aggregation. They’re like little windows, not into what the system has collected about users, but into what the system has inferred about them. However, even targeted ads on Google were perceived to only reveal information that the user already gave to Google: the search query. Google may simultaneously provide both a greater feeling of control (over what search terms are entered and what happens when links are clicked), and less feedback that data aggregation is taking place (via the perception that ads are only related to search terms, not profiles). The main difference between social versus information privacy is the behind-the-scenes aggregation and analysis that is pervasive when interacting with systems, but that does not take place when interacting with other people. The individual bits of information we reveal mean something different, in isolation, than they do as part of a processed aggregate. The invisibility of the infrastructure, from the users’ perspective, is both blessing and curse: personalization holds the promise of better usability and access to information, but at the same time the fact that we can’t see it makes it harder for us to understand its implications.”

2015

Title Privacy and human behavior in the age of information	
published in Science, 30 January 2015: Vol. 347 no. 6221 pp. 509-514	
Year 2015	Authors Alessandro Acquisti, Laura Brandimarte, George Loewenstein
Setting of the experiment "This Review summarizes and draws connections between diverse streams of empirical research on privacy behavior." The authors use "three themes to connect insights from social and behavioral sciences: people's uncertainty about the consequences of privacy-related behaviors and their own preferences over those consequences; the context-dependence of people's concern, or lack thereof, about privacy; and the degree to which privacy concerns are malleable — manipulable by commercial and governmental interests."	
Research question "Are individuals up to the challenge of navigating privacy in the information age?"	
Results *(copied from abstract/conclusions of the publication)* "Uncertainty and context-dependence imply that people cannot always be counted on to navigate the complex trade-offs involving privacy in a self-interested fashion. People are often unaware of the information they are sharing, unaware of how it can be used, and even in the rare situations when they have full knowledge of the consequences of sharing, uncertain about their own preferences." Additionally, "the rules people follow for managing privacy very by situation, are learned over time, and are based on cultural, motivational, and purely situational criteria." Malleability, in turn, implies that people are easily influenced in what and how much they disclose. Moreover, what they share can be used to influence their emotions, thoughts, and behaviors in many aspects of their lives, as individuals, consumers, and citizens. Although such influence is not always or necessarily malevolent or dangerous, relinquishing control over one's personal data and over one's privacy alters the balance of power between those holding the data and those who are the subjects of that data. Insights from the social and behavioral empirical research on privacy reviewed here suggest that policy approaches that rely exclusively on informing or "empowering" the individual are unlikely to provide adequate protection against the risks posed by recent information technologies. Consider transparency and control, two principles conceived as necessary conditions for privacy protection. The research […] shows that they may provide insufficient protections and even backfire when used apart from other principles of privacy protection. The research	

reviewed here suggests that if the goal of policy is to adequately protect privacy (as we believe it should be), then we need policies that protect individuals with minimal requirement of informed and rational decision-making— policies that include a baseline framework of protection, such as the principles embedded in the so-called fair information practices. People need assistance and even protection to aid in navigating what is otherwise a very uneven playing field. […] a goal of public policy should be to achieve a more even equity of power between individuals, consumers, and citizens on the one hand and, on the other, the data holders such as governments and corporations that currently have the upper hand. To be effective, privacy policy should protect real people — who are naïve, uncertain, and vulnerable — and should be sufficiently flexible to evolve with the emerging unpredictable complexities of the information age."

Title Call for information - The commercial use of consumer data	
published in CMA – Competition & Markets Authority UK	
Year 2015	Authors CMA – Competition & Markets Authority
Setting of the experiment Questionnaire for companies to find out how consumer data are commercially used.	
Research question How are consumer data commercially used?	
Results *(copied from abstract/conclusions of the publication)* No results published yet.	

Title Readability of Privacy Policies of Healthcare Websites	
published in in: Thomas. O.; Teuteberg, F. (Hrsg.): Proceedings der 12. Internationalen Tagung Wirtschaftsinformatik (WI 2015), Osnabrück, S. 1085-1099	
Year 2015	Authors Tatiana Ermakova, Benjamin Fabian, and Eleonora Babina

Setting of the experiment They “retrieved a set of 5,234 unique DMOZ health websites' privacy policies together with their DMOZ categories and added the 197 mobile health apps’ policies to the database as the category “Mobile”. [Their] final sample consisted of 5,431 privacy policies covering various healthcare areas which involved Medicine, Conditions and Diseases, Animal, Mental Health, Alternative, Public Health and Safety, Mobile, Addictions, Pharmacy, Nursing, Reproductive Health, Professions, Dentistry, Senior Health, and others. Additionally, another set of 1166 privacy policies of Alexa top e-commerce websites was collected. For the purpose of analysis, we imported the resulting reports into the R environment for statistical computing.”
Research question Examination of the readability “of privacy statements of healthcare websites and […] their efficiency to communicate their attitudes regarding consumers’ privacy which influence the formation of consumers’ behavior”
Results *(copied from abstract/conclusions of the publication)* The authors “investigated the readability of a large and representative number of privacy policies of healthcare websites in general and in groups, as well as in comparison to top commercial websites. Privacy policies in the healthcare domain are difficult to read, what is consistent with prior research. They contain a mean of slightly more than 1,000 words. On average, a reader is expected to be educated at the college level, to have the 13th reading grade level or be 16 years formally educated. Healthcare websites provide shorter and in general more readable privacy policies than top e-commerce websites. Commercial and non-commercial healthcare websites have identically long privacy policies, although the policies of commercial healthcare websites are more readable.” Their “results imply that in terms of their readability, privacy statements of current healthcare websites do not appropriately communicate their attitude regarding consumers’ privacy on the website and do not positively influence the formation of consumers’ behavior. Healthcare websites’ providers, especially those working on a non-commercial basis, should make serious efforts to rewrite these statements. In particular, improving privacy policies should be a concern to non-commercial healthcare but also top e-commerce website providers.”

Title Your Location has been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging
published in CHI 2015, April 18 - 23 2015, Seoul, Republic of Korea.

Year	Authors
2015	Almuhimedi, H.; Schaub,F.; Sadeh, N.; Adjerid, I.; Acquisti, A.; Gluck, J.; Cranor, L.; Agarwal, Y.

Setting of the experiment

The authors "conducted a field study to gain insights on the effect and perceived utility of mobile privacy managers, as well as the effect and perception of privacy nudges." They "designed a mobile privacy nudge that provides concise privacy-relevant information and meaningful actions that reduce the threshold for users to act upon the nudge's content."

The "field study consisted of an entry session, three consecutive field phases lasting 22 days in total, an exit survey, and an optional exit interview."

The study itself was conducted from "May to July 2014". "Participants were recruited via Craigslist and from a city-wide participant pool maintained" by the authors university. […] Twenty-six respondents, meeting the following criteria, were invited to participate in the study: (1) Adults who have Android phones running Android version 4.3–4.4 (because AppOps is only supported by these Android versions); (2) have a mobile data plan with at least 2GB/month (as data would have to be transferred during the study); (3) able to visit our lab for the entry session. Three were later disqualified […]."

Research question

The study focuses on two research questions: "(1) Is access to a fine-grained app permission manager an effective way of helping users review and modify their app permissions? (2) Can privacy nudges, that regularly alert users about sensitive data collected by their apps, enhance the effectiveness of a fine-grained app permission manager?"

Results

"In summary, results from [the] study indicate that Android users benefit from an app permission manager such as App Ops, with a majority of our participants taking advantage of the controls it offers. They also indicate that, even with access to such a manager, user's awareness of the data collected by their apps remains limited. Users would further benefit from receiving nudges that inform them about the sensitive data collected by their apps. The nudges used in this study were fairly simplistic. Moving forward, nudges would benefit from possibly being further personalized, salient, sticky, and configurable but not annoying."

References

Abadie, A. and Gay, S. (2006): The impact of presumed consent legislation on cadaveric organ donation: A cross-country study. Journal of Health Economics 25(4): 599-620.

Acar, G.; Eubank, C.; Engelhardt, S.; Juarez, M.; Narayanan, A. and Diaz, C. (2014): The Web never forgets: Persistent tracking mechanisms in the wild. Proceedings of CCS 2014, Nov. 2014.

Acquisti, A.; Brandimarte, L.; Loewenstein, G. (2015): Privacy and human behavior in the age of information. Science 347(6221): 509-514

Acquisti A., Grossklags J. (2005): Privacy and rationality in individual decision making. IEEE Security & Privacy 3(1) 26-33.

Acquisti A.; Grossklags J. (2007): What Can Behavioral Economics Teach Us About Privacy?, in Acquisti A et al. (eds), Digital Privacy: Theory, Technologies and Practices. Auerbach Publications, Taylor and Francis Group.

Acquisti, A. (2009): Nudging Privacy. The Behavioral Economics of Personal Information. Security & Privacy Economics IEEE (November/December 2009): 72-75 (pre-publication version).

Acquisti, A. (2010): The Economics of Personal Data and the Economics of Privacy. Background Paper No. 3, Joint WPISP-WPIE Roundtable: "The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines", 1 December 2010.

Acquisti, A.; Adjerid, I.; Brandimarte, L. (2013): Gone in 15 Seconds: The Limits of Privacy Transparency and Control. Security & Privacy, IEEE 11(4): 72-74.

Acquisti, A.; Grossklags, J. (2004): Privacy Attitudes and Privacy Behavior. Gains, Losses and Hyperbolic Discounting. In Camp, J. and Lewis, R. (Eds.): The Economic of Information Security. Berlin, Kluwer.

Ægis (2014): M2M application characteristics and their implications for spectrum. Final report, 2606/OM2M/FR/V2: 1-78. Available at: http://stakeholders.ofcom.org.uk/binaries/research/technology-research/2014/M2M_FinalReportApril2014.pdf

Aïmeur, E.; Brassard, G.; Rioux, J. (2013): Data Privacy: An End-User Perspective. International Journal of Computer Networks and Communications Security. VOL.1, NO.6, November 2013, 237–250.

Ammar, W.; Wilson, S.; Sadeh, N.; Smith, N.A. (2012): Automatic Categorization of Privacy Policies: A Pilot Study. School of Computer Science, Carnegie Mellon University PA 15213.

Almuhimedi, H.; Schaub, F.; Sadeh, N.; Adjerid, I.; Acquisti, A.; Gluck, J.; Cranor, L.; Agarwal, Y. (2015): Your Location has been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging. CHI 2015, April 18 - 23 2015, Seoul, Republic of Korea: 1-10.

Ariely, D. (2008): Predictably Irrational: The Hidden Forces that Shape Our Decisions. Harper: London.

Arnold, R.; Waldburger, M. (2014): The Impact of Data on ICT Business Models. GSR Discussion Paper. Available at: http://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2014/GSR14%20Impact_of_dataBusinessModels.pdf.

Article 29 Data Protection Working Party (2014): Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting. 14/EN WP 224: 1-11.

Article 29 Working Party (2012), Letter to Google. 16.10.2012.

Article 29 Working Party, „Opinion 04/2012 on Cookie Consent Exemption“ (WP 194) 7 June 2012.

Article 29 Working Party, „Opinion 10/2004 on more harmonised information provisions“ (WP 100), 25 November 2004.

Article 29 Working Party, „Opinion 15/2011 on the definition of consent“ (WP 187) 13 July 2011.

Article 29 Working Party, „Opinion 8/2014 on the Recent Developments on the Internet of Things“ (WP 2234) 16 September 2014.

Ayres I. (2012): Regulating Opt Out: An Economic Theory of Altering Rules. 121 Yale L.J. 2032 (2012).

Ayres, I.; Schwartz, A. (2014): The No Reading Problem in Consumer Contract Law, Stanford Law Review 2014: 545-600.

Bakos, Y.; Marotta-Wurgler, F.; Trossen, D.R. (2009): Does Anyone Read the Fine Print? Consumer Attention to Standrad Form Contracts. NYU Law and Economics Research Paper No. 09-40.

Balebako, R.; Leon, P.G.; Almuhimedi, H.; Kelley, P.G.; Mugan, J.; Acquisti, A.; Cranor, L.F.; Sadeh, N. (2011): Nudging users towards privacy on mobile devices. Proc. CHI 2011 Workshop on Persuasion, Nudge, Influence and Coercion.

Bansal, G.; Zaledi, F. and Gefen, D. (2008): Efficacy of Privacy Assurance Mechanisms in the Context of Disclosing Health Information Online. AMCIS Proceedings. Paper 178.

Bansal, G.; Zaledi, F. and Gefen, D. (2008): The Moderating Influence of Privacy Concern on the Efficacy of Privacy Assurance Mechanisms for Building Trust: A Multiple-Context Investigation. ICIS Proceedings Paper 7.;

Barnes, W. R. (2012): Social Media and the Rise in Consumer Bargaining Power. University of Pennsylvania, Journal of Business Law (Vol. 14:3 2012): 661-699.

Barocas, S.; Nissenbaum, H. (2009): On Notice: The Trouble with Notice and Consent. Proceedings of the Engaging Data Forum. The First International Forum on the Application and Management of Personal Electronic Information.

Bashir, M.; Hoff, K.A.; Hayes, C.M.; Kesan, J.P. (2014): Knowledge-based Individualized Privacy Plans (KIPPs): A Potential Tool to Improve the Effectiveness of Privacy Notices”, Workshop on the Future of Privacy Notice and Choice, Carnegie Mellon University June 27, 2014.

Becher, S. L. Unger-Aviram, E. (2010): The Law of Standard Form Contracts: Misguided Intuitions and Suggestions for Reconstruction. DePaul Business & Commercial Law Journal, Vol. 8: 199-227.

Beese, J. (2012): Facebook Removes „Privacy“ From New Data Use Policy. SproutScoial 23-03-2012. Available at: http://sproutsocial.com/insights/facebook-data-use-policy/

Bellman, S., Johnson, E.J., Kobrin, S. J., Lohse, G.L. (2004): International Differences in Information Privacy Concerns: A Global Survey of Consumers, The Information Society, 20: 313–324.

Better Regulation Executive and National Consumer Council (2007): Warning: Too much information can harm. A final report by the Better Regulation Executive and National Consumer Council on maximising the positive impact of regulated information for consumers and markets. London.

Birrell, E.; Schneider, F. B. (2014): Fine-Grained User Privacy from Avenance Tags. Computing and Information Science Technical Reports. Department of Computer Science, Cornell University.

Böhme, R. and Köpsell, S. (2010): Trained to Accept? CHI '10 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Atlanta, Georgia, USA: 2403-2406

Brandimarte, L.; Acquisti, A.; Loewenstein, G. (2010): Misplaced Confidences: Privacy and the Control Paradox. Ninth Annual Workshop on the Economics of Information Security (WEIS). June 7-8 2010

Buller, D.B. (1986): Distraction during persuasive communication: A meta-analytic review. Communication Monographs 53: 91-114.

Bygrave L. A. (2014): Data privacy law. An international perspective. Oxford University Press.

Cadogan, R.A. (2004): An Imbalance of Power: The Readability of Internet Privacy Policies. Journal of Business and Economic Research 2(3): 49-62.

Castelluccia, C.; Kaafar, M.A.; Tran, M.-D. (2012): Betrayed by Your Ads! Reconstructing User Profiles From Targeted Ads. Privacy Enhancing Technologies – Lecture Notes in Computer Science Vol. 7384: 1-17.

Choe, E. K.; Jung, J.; Lee, B.; Fisher, K. (2013): Nudging people away from privacy-invasive mobile apps through visual framing. Human-Computer Interaction–INTERACT. Springer.

CMA – Competition & Markets Authority UK (2015): Call for information - The commercial use of consumer data. London.

Coase, R.H. (1960): The Problem of Social Cost. ournal of Law and Economics. Vol. 3 (Oct., 1960): 1-44

Coopamootoo, P.L.; Ashenden, D. (2011): Designing usable online privacy mechanisms: what can we learn from real world behaviour?. Privacy and Identity Management for Life. IFIP Advances in Information and Communication Technology (Volume 352): 311-324.

Council for International Organizations of Medical Sciences (2002): International Ethical Guidelines for Biomedical Research Involving Human Subjects.

Court of Justice of the European Union, Case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos and Mario Costeja González.

Cranor, L. F.; Hoke, C.; Leon, P. G.; Au, A. (2014): Are They Worth Reading? An In-Depth Analysis of Online Advertising Companies' Privacy Policies. Non-reviewed draft paper presented at the 42nd Research Conference on Communication, Information and Internet Policy (TPRC 2014).

Cranor, L.F. (2003): 'I didn't Buy it for Myself': Privacy and Ecommerce Personalization. Proceedings of the ACM Workshop on Privacy in the Electronic Society, Washington, DC, October 30.

Custers, B.; van der Hof, S.; Schermer, B.; Appleby-Arnold, S.; Brockdorff, N. (2013): Informed Consent in Social Media Use – The Gap between User Expectations and EU Personal Data Protection Law. Oben access article published in SCRIPTed.

D21 Initiative (Ed.) (2014): D21-Digital-Index 2014. Die Entwicklung der digitalen Gesellschaft in Deutschland. Berlin.

Datta, A.; Tschantz, M. C.; Datta, A. (2014): Automated Experiments on Ad Privacy Settings: A Tale of Opacity, Choice, and Discrimination. Proceedings of Privacy Enhancing Technologies Symposium, July 2014.

De Geest, G. (2002). The signing-without- reading problem: An analysis of the European Directive on unfair contract terms, in H. B. Schäfer & H. J. Lwowski (Eds.), Konsequenzen wirtschaftsrechtlicher Normen Festschrift für Klaus Ott (pp. 213–235). Wiesbaden: Gabler.

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 (Directive on privacy and electronic communications). Official Journal L 201 , 31/07/2002 P. 0037 – 0047.

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. Official Journal L 281 , 23/11/1995 P. 0031 – 0050.

Doherty, C. and Lang, M. (2014): An Exploratory Survey of the Effects of Perceived Control and Perceived Risk on Information Privacy. 9th Annual Symposium on Information Assurance (ASIA'14), June 3-4, 2014, Albany, NY: 23-28.

Doty, N. and Gupta, M. (2013): Privacy Design Patterns and Anti-Patterns. Symposium On Usable Privacy and Security (SOUPS) 2013, A Turn for the Worse: Trustbusters for User Interfaces Workshop: 1-5.

Drèse, X., Hussherr, F.-X. (2003): Internet advertising: Is anybody watching? Journal of Interactive Advertising 17(4): 8-23.

Dreyer, S.; Ziebrath, L. (2014): Participatory Transparency in Social Media Governance: Combining two Good Practices. Journal of Information Policy, Vol. 4, 2014: 529-546.

Eckersley, P. (2010): How Unique Is Your Web Browser? Privacy Enhancing Technologies. Lecture Notes in Computer Science, Volume 6205: 1-18.

ECtHR, Copland v. United Kingdom, No. 62617/00, 3 April 2007, par 44.

Edwards, L., Abel, W. (2015): The Use of Privacy Icons and Standard Contract Terms for Generating Consumer Trust and Confidence in Digital Services. CREATe Working Paper 2014/15.

Egelman, S.; Tsai, J.; Cranor, L.F., Acquisti, A. (2009): Timing is Everything? The Effects of Timing and Placement of Online Privacy Indicators. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems: 319-328.

Epp, C.; Lippold, M. and Mandryk, R.L. (2011): Identifying emotional states using keystroke dynamics. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems: 715-724.

Ermakova, T.; Baumann, A.; Fabian, B.; Krasnova, H. (2014): Privacy Policies and Users' Trust: Does Readibility Matter? Proceedings of the Americas Conference on Information Systems (AMCIS, Savannah, USA).;

Ermakova, T.; Fabian, B. and Babina, El (2015): Readability of Privacy Policies of Healthcare Websites. Thomas, O. and Teuteberg, F. (Eds.): Proceedings der 12. Internationalen Tagung Wirtschaftsinformatik (WI 2015). Osnabrück: 1085-1099.

Eubank, C.; Melara, M.; Perez Botero, D.; Narayanan, A. (2013): Shining the Floodlights on Mobile Web Tracking – A Privacy Study. Proceedings of the IEEE Workshop on Web 2.0.

European Commission, „Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), COM(2007)228 final, Brussels, 2 May 2007.

European Commission, „Special Eurobarometer 359: Attitudes on data protection and electronic identity in the European Union" (2011).

European Consumer Centre Ireland (2008): Car Rental Contracts: Business practices, contract terms and consumer protection. Dublin.

European Consumer Centres Network - ECC-net (2013): Trust marks report 2013 "Can I trust the trust mark?"

Federal Trade Commission (2015): Internet of Things. Privacy & Security in a Connected World. FTC Staff Report: 1-55

Feldman, L.; Turow, J.; Meltzer, K. (2005): Open to Exploitation: American Shoppers Online and Offline. Annenberg Public Policy Center.

Fransen, M.L.; Verlegh, P.W.J.; Kirmani, A. and Smit, E.G. (2015): A typology of consumer strategies for resisting advertising, and a review of mechanisms for countering them. International Journal of Advertising 34(1): 6-16.

Gartner (2014): Gartner's 2014 Hype Cycle for Emerging Technologies Maps the Journey to Digital Business. Press release.

Godes, D. and Mayzlin, D. (2004): Using online conversations to study word-of-mouth communication. Marketing Science 23(4): 545-560.

Goldstein, D.G.; Johnson, E.J.; Hermann, A. and Heitmann, M. (2008): Nudge your customers towards better choices. Harvard Business Review 86(12): 99-105.

Good, N.; Grossklags, J., Thaw, D.; Perzanowski, A.; Mulligan, D. K.; Konstan, J. (2006): User Choices and Regret: Understanding Users' Decision Process about Consensually Acquired Spyware. A Journal Of Law And Policy For The Information Society, Issue (2006): 283-344.

Greenleaf, G. (2013): Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories. Journal of Law, Information & Science 23(1).

Halle, T. (2014): What You Think You Know About the Web Is Wrong. TIME 03-09-2014.

Hart, H. (1961): The Concept of Law. Clarendon Press.

Helberger, N. (2013): Form Matters: Informing Consumers Effectively. Amsterdam Law School Research Paper No. 2013-71/Institute for Information Law Research Paper No. 2013-10.

Helberger, N. (2013): Freedom of Expression and the Dutch Cookie-Wall. Amsterdam Law School Research Paper No. 2013-66/Institute for Information Law Research Paper No. 2013-06.

Helberger, N.; Eijk N. van; Kool, L.; van der Plas, A.; an der Sloot, B. (2012): Online tracking: questioning the power of informed consent", info, Vol. 14 Iss: 5, pp.57 – 73.

Högberg, J. (2013): The effect of effort, control and value frames on online users privacy decision. Master Thesis at the Faculty of Ecnomic Sciences, Communication and IT. Karlstad University.

Hoofnagle, C.J. and King, J. (2007): Consumer Information Sharing: Where the Sun Still Don't Shine. University of California, Berkeley.

Hoofnagle, C.J. et al (2012): Behavioral Advertising: The Offer You Cannot Refuse. 6(2) Harvard Law & Policy Review 273: 273-296.

Hoofnagle, C.J.; Good, N. (2012): The web privacy census (October 2012) http://law.berkeley.edu/privacycensus.htm.

Hoofnagle, C.J.; King, J. (2008): What Californians Understand about Privacy Online (UC Berkeley). 3 September 2008. Research Report.

Hoofnagle, C. J.; Whittington, J.M. (2014): Free: Accounting for the Costs of the Internet's Most Popular Price. UCLA Law Review 61 (606): 608-670.

Howells, G. (2005): The Potential and Limits of Consumer Empowerment by Information. Journal of Law and Society 32(3): 349-370.

Hui, K.L.; Teo, H.H. and Lee, S.Y.T. (2007): The Value of Privacy Assurance: An Exploratory Field Experiment. MIS Quarterly 31: 19-33.

IAB (2014): Facebook fails on advertising front but scores as branding platform, says iLead. Available at: http://iabsa.net/research-data/facebook-fails-on-the-advertising-front-but-scores-points-as-branding-platform-ilead/

Information Commissioner's Office (2013): Direct marketing. Data Protection Act. Privacy and Electronic Communications Regulations. Version 1.1, p 1-44.

Interactive Advertising Bureau United Kingdom, „Department for Business, Innovation & Skills consultation on implementing the revised EU electronic communications framework, IAB UK Response" (1 December 2012) www.iabuk.net/sites/default/files/IABUKresponsetoBISconsultationonimplementingtherevisedEUElectronicCommunicationsFramework_7427_0.pdf, p 2.

International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use (1996): Guideline for Good Clinical Practice. ICH Harmonised Tripartite Guideline, E6(R1): 1-59.

International Covenant on Civil and Political Rights

Irion, K.; Luchetta, G. (2013): Online Personal Data Processing and EU Data Protection Reform. CEPS Task Force Report of the CEPS Digital Forum 2013.

Irish Statutory Instrument (S.I.) No. 535 of 2003 as amended by S.I. No. 526 of 2008 www.dataprotection.ie/viewdoc.asp?DocID=896.

Iyengar, S.S.; Lepper, M.R. (2000): When Choice is Demotivating: Can One Desire Too Much of a Good Thing?. Journal of Personality and Social Psychology. Vol. 79, No. 6: 995 -1006.

Jacks, J. Z. and Cameron, K. A. (2003): Strategies for resisting persuasion. Basic and Applied Social Psychology 25(2): 145-161.

Jensen, C.; Potts, C. (2004): Privacy policies as decision-making tools: an evaluation of online privacy notices. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems: 471-478.

Jensen, C.; Potts, C.; Jensen, C. (2005): Privacy Practices of Internet Users: Self-Reports versus Observed Behavior. International Journal of Human-Computer Studies 63: 203-227.

Jin, L. (2011): Improving response rates in web surveys with default setting: The effects of default on web survey participation and permission. International Journal of Advertising 53(1): 75-94.

Johnson, E.J., Goldstein, D. (2003): Do Defaults Save Lives?. Science 302(5649): 1338-1339.

Kelly, L.M.V. (2014): An Exploration of Advertising Engagement, Advertising Avoidance and Privacy Concerns on Social Networks Sites. PhD Thesis at the School of Advertising, Marketing and Public Relations – QUT Business School. Queensland University of Technology – November 2014.

Kim, N. (2010): Wrap Contracts and Privacy. Association for the Advancement of Artificial Intelligence. Press Technical Report SS-10-05.

Kleimann Communication Group (2006): Evolution of a Prototype Financial Privacy Notice. A Report on the Form Development Project.

LaRose, R.; Rifon, N.J. (2007): Promoting i-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior. The Journal of Consumer Affairs 41(1): 127-149.

Li, H.; Sarathy, R.; Xu, H. (2011): The Role of Affect and Cognition on Online Consumers' Decision to Disclose Personal Information to Unfamiliar Online Vendors. Decision Support Systems 51: 434-445.

Localytics (2014): App Rentention Improves – Apps Used Only Once Declines to 20%. 06-11-2014. Available at: http://info.localytics.com/blog/app-retention-improves

Luth, H. A. (2010): Behavioural Economics in Consumer Policy: The Economic Analysis of Standard Terms in Consumer Contracts Revisited (PhD thesis University of Rotterdam) (Academic version 2010).

Maronick, T. J. (2014): Do Consumers Read Terms of Service Agreements When Installing Software? A Two-Study Empirical Analysis. International Journal of Business and Social Research 4(6): 137-145.

Massey, A. K.; Eisenstein, J.; Anton, A. I., Swire, P.P. (2013): Automated Text Mining for Requirements Analysis of Policy Documents. Requirements Engineering Conference (RE), 2013 21st IEEE International: 4-13.

McDonald, A. M.; Cranor, L. F. (2008): The Cost of Reading Privacy Policies. A Journal of Law and Policy for the Information Society 4(3) I/S: 540.

McDonald, A. M.; Cranor, L. F. (2010): Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising (38th Research Conference on Communication, Information and Internet Policy, Telecommunications Policy Research Conference) (2 October 2010).

McDonald, A.M.; Reeder, R.W.; Kelley, P.G. and Cranor, L.F. (2009): A Comparative Study of Online Privacy Policies and Formats. Privacy Enhancing Technologies – Lecture Notes in Computer Science 5672: 37-55

Meirick, P. (2002): Cognitive responses to negative and comparative political advertising. Journal of Advertising 31(1): 49-62.

Milne, G.R.; Culnan, M.J. (2004): Strategies for Reducing Online Privacy Risks: Why Consumers Read (or don't Read) Privacy Notices. Journal of Interactive Marketing (18): 15-29.

Mitts, J. (2014): How Effective is Mandatory Disclosure?. Columbia University. Working paper.

Moores, T. (2005): Do Consumers Understand the Role of Privacy Seals in E-Commerce?. Communications of the ACM 8648(3): 89-90.

Mowery, K.; Bogenreif, D.; Yilek, S.; Shacham, H. (2011): Fingerprinting information in JavaScript implementations. Proceedings of Web 2.0 Security & Privacy (W2SP) 2011. IEEE Computer Society: 1-11.

Mowery, K.; Shacham, H. (2012): Pixel Perfect: Fingerprinting Canvas in HTML5. Proceedings of Web 2.0 Security & Privacy (W2SP) 2012. IEEE Computer Society: 1-12.

Nehf, J. P. (2007): Shopping for Privacy Online: Consumer Decision Making Strategies and the Emerging Market for Information Privacy. The Journal of Consumer Affairs, Vol. 41(2): 351-375.

Nest (2015): Install it yourself. Available at: https://nest.com/thermostat/installation/#thermostat-diy-installation

Nikiforakis, N.; Kapravelos, A.; Joosen, W.; Kruegel, C.; Piessens, F.; Vigna, G. (2013): Cookieless Monster: Exploring the Ecosystem of Web-based Device Fingerprinting. 2013 IEEE Symposium on Security and Privacy: 1-15.

Nissenbaum, H. (2011): A Contextual Approach to Privacy Online. Daedalus 140(4): 32-48.

Ofcom (2013): A Review of Consumer Information Remedies. Research Dokument, 12th March 2013. London.

Orito, Y.; Murata, K. and Fukuta, Y. (2013): Do online privacy policies and seals affect corporate trustworthiness and reputation? International Review of Information Ethics 19(7): 52- 65.

Petty and Cacioppo (1983) [Cacioppo, J. T., & Petty, R. E. (1983). Social psychophysiology: A sourcebook. New York: Guildford Press.]

Phoenix Strategic Perspectives (2013): Survey of Canadians on Privacy-Related Issues. Prepared for the Office of the Privacy Commissioner of Canada.

Presidential Commission for the Study of Bioethical Issues (2014): Informed Consent Background: 1-17.

Proposal for a Data Protection Regulation, consolidated version after LIBE Committee vote, 22 October 2013, www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf.

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) Brussels, 25.1.2012 COM(2012) 11 final.

Rader, E. (2014): Awareness of Behavioral Tracking and Information Privacy Concern in Facebook and Google. Symposium on Usable Privacy and Security (SOUPS) 2014, July 9–11,2014, Menlo Park, CA.

Rao, A.; Schaub, F. Sadeh, N. (2014): What do they know about me? Contents and Concerns of Online Behavioral Profiles. 2014 ASE BigData/SocialInformatics/PASSAT/BioMedCom 2014 Conference, Harvard University, December 14-16, 2014.

Rejón-Guardia, F.; Sánchez-Fernández, J.; and Muñoz-Leiva, F. (2014): A Generalization of Advertising Avoidance Model on Social Network. Working Paper in Review.

Rich, J. (2015): Beyond Cookies: Privacy Lessons for Online Advertising. AdExchanger Industry Preview 01-21-2015, available at: https://www.ftc.gov/system/files/documents/public_

Richard H. Thaler, R.H.; Sunstein, C.R. (2003): Libertarian Paternalism, 93 American Economic Review 175 (May 2003): 175-179.

Richie, A.; Corrigan, J.; Graham, S.; Hague, A.; Higham, A.; Holt, J.; Mowbray, P. (2011): Transforming consumer information A study conducted by the Consumer Information Working Party, 26 October 2011, Working paper

Rowan, M. and Dehlinger, J. (2014): A privacy policy comparison of health and fitness related mobile applications. Procedia Computer Science 37(2014): 348-355.

Sadeh, N.; Acquisti, A.; Breaux, T.D.; Cranor, L.F.; McDonald, A.M. Joel R. Reidenberg, J.R.; Smith, N.A.; Liu, F., Russell, N.C.; Schaub, F.; Wilson, S. (2013): The Usable Privacy Policy Project: Combining Crowdsourcing, Machine Learning and Natural Language Processing to Semi-Automatically Answer Those Privacy Questions Users Care About. December 2013, Research paper CMU-ISR-13-119.

Saevanee, H. and Bhattarakosol, P. (2009): Authenticating User Using Keystroke Dynamics and Finger Pressure. Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE.

Samuelson, W.; Zeckhauser, R. (1988): Status Quo Bias in Decision Making. Journal of Risk and Uncertainty. Volume 1(1): 7-59

Sarode, S. (2014): Opportunity cost analysis of android smartphones' permissions. Master Thesis at the Rutgers University New Brunswick.

Schoenheit, I. (2004): Was Verbraucher wissen wollen. Ergebnisse und Thesen zu einer empirischen Studie. Verbraucherzentrale Bundesverband vzbv (eds.). Berlin.

Shah, R. C. and Sandvig, C. (2008): Software Defaults as de facto Regulation: The case of the wireless internet. Information, Communication & Society 11(1): 25-46.

Shapiro, C.; Varian, H.R. (1999): Information Rules. A Strategic Guide to the Network Economy. Harvard Business School Press.

Speck, P. S.; Elliot, M. (1997): Predictors of advertising avoidance in print and broadcast media. Journal of Advertising 26(3): 61-76.

Stark, J. K.; Choplin, J. M. (2009): A License to Deceive: Enforcing Contractual Myths Despite Consumer Psychological Realities. 5 N.Y.U. J. L. & Bus: 617-744.

Strandburg, K. J. (2013): Free Fall: the Online Market's Consumer Preference Disconnect. New York University Law and Economics Working Papers. Paper 354.

Sultan, F., Urban, G.L.; Shankar, V. and Bart, I.Y. (2002): Determinants and Role of Trust in e-Business. A Large Scale Empirical Study. MIT Sloan School of Management.

Sunstein, C. R. (2013): Deciding By Default. University of Pennsylvania Law Review 162(1): 1-57.

Sunstein, C. R.; Thaler, R. H. (2008): Nudge: Improving Decisions about Health, Wealth, and Happiness. Yale University Press.

Thaler, R. H.; Tucker, W. (2013): Smarter Information, Smarter Consumers. Harvard Business Review, January-February: 44-54.

The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research (1978): The Belman Report. Ethical Principles and Guidelines for the Protection of Human Subjects of Research: 1-40.

The Task Force on Smart Disclosure: Information and Efficiency in Consumer Markets (2013): Smart Disclosure and Consumer Decision Making: Report of the Task Force on Smart Disclosure.

Traung, P. (2012): The Proposed New EU General Data Protection Regulation: Further Opportunities. Computer Law Review international 2012(2): 33-49.

Tsai, J.Y.; Egelman, S.; Cranor, L.; Acquisti, A. (2011): The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. Information Systems Research 22: 254-268.

Turow, J. (2001): Privacy Policies on Children's Websites: Do They Play by the Rules? The Annenberg Public Policy Center, March 2001.

Turow, J. (2011): The Daily You: How the New Advertising Industry is Defining Your Identity and Your Worth. Yale University Press 2011.

Turow, J.; Hoofnagle; C. J.; Mulligan, D. K.; Good, N.; Grossklags, J. (2007): The Federal Trade Commission and Consumer Privacy in the Coming Decade. A Journal of Law & Policy for the Information Society 3(3) I/S: 723-749.

Turow, J.; Mulligan, D.K. and Hoofnagle, C.J. (2007): Research Report: Consumers Fundamentally Misunderstand the Online Advertising Marketplace. Samuelson Law, Technology, & Public Policy Clinic/Annenberg Public Policy Center.

UN Declaration of Human Rights.

Ur, B.; Leon, P.G.; Cranor, L. F.; Shay, R.; Wan, Y. (2012): Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising. Proceedings of the Eighth Symposium on Usable Privacy and Security ACM.

Verbraucherzentrale Bundesverband (vzbv) (2011): Information gut, alles gut? Berlin.

Vila, T.; Greenstadt, R.; Molnar, D. (2004): Why We Can't be Bothered to Read Privacy Policies. Models of Privacy Economics as a Lemons Market. Proceeding ICEC '03 Proceedings of the 5th international conference on Electronic commerce: 403-407

Wagenaar, R.W. and Eldin A.M.T. (2003): Towards a Component Based Privacy Protector Architecture. Proceedings 15th Conference On Advanced Information Systems Engineering – Klagenfurt, Oostenrijk: 1-11.

Wang, Y.; Leon, P. G.; Acquisti, A.; Cranor, L. F.; Forget, A.; Norman Sadeh, N. (2014): A Field Trial of Privacy Nudges for Facebook. CHI 2014 , Apr 26 – May 01 2014, Toronto, ON, Canada, ACM 978-1-4503-2473-1/14/04.

Wang, Y.; Leon, P. G.; Chen, X.; Komanduri, S.; Norcie, G. Scott, K.; Acquisti, A.; Cranor, L. F.; Norman, S. (2013): The Second Wave of Global Privacy Protection: From Facebook Regrets to Facebook Privacy Nudges. Ohio State Law Journal, 74 (2013): 1307-1335.

Waters, R.; Bradshaw, T. (2015): Google suspends sale of smartglasses. Available at: http://www.ft.com/cms/s/0/ff12af46-9ce8-11e4-adf3-00144feabdc0.html

Wauters, E.; Lievens, E.; Valcke, P. (2013): D1.2.4: A legal analysis of Terms of Use of Social Networking Sites, including a practical legal guide for users: 'Rights & obligations in a social media environment. iMinds-ICRI – KU Leuven.

Webber, M.; Harris, T.; Jones, M. (2009): Better Information Handbook. Advice Services Alliance. London.

WHO (2002): International Ethical Guidelines for Biomedical Research Involving Human Subjects. Prepared by the Council for International Organizations of Medical Sciences (CIOMS) in collaboration with the World Health Organization (WHO). Geneva: 33.

Wilkinson-Ryan, T. (2014): A Psychological Account of Consent to Fine Print. Institute for Law and Economics at the University of Pennsylvania, Research Paper No. 14-22.

Willis, L. E. (2013): Why Not Privacy by Default?. Berkeley Technology Law Journal 29 (61): 121-128.

World Medical Association (2013): WMA Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects. 7th revision.

Zuiderveen Borgesius, F. J. (2015): Improving Privacy Protection in the Area of Behavioural Targeting (PhD thesis University of Amsterdam), Kluwer law International (forthcoming).

Zuiderveen Borgesius, F. (2015): Behavioural Sciences and the Regulation of Privacy on the Internet Nudging and the Law - What can EU Law learn from Behavioural Sciences?'. Sibony A-L, . Alemanno, A., eds. (forthcoming).

Glossary

Digital Natives	Persons brought up in the digital age.
Framing Effect	A concept stating that formally identical decision problems can result in different decisions depending on their presentation. This concept was first introduced by Kahneman and Tversky (1981).
Canvas element	An area defined in HTML code with height and width attributes. It allows scriptable rendering. JavaScript code is used to draw in the canvas element.
Evercookies	Evercookies are a special form of persistent cookies. They are stored on several locations on a user's computer.
Deep Packet Inspection (DPI)	When data is sent over packet-switched computer networks, such as over the Internet, data is split into small packets, which are routed individually from sender to destination. For the routing to work, overhead information is added to each data packet. This is comparable to letters mailed by post. The letter's content is wrapped in an envelope giving the postal service all relevant information to forward and deliver the letter to its destination. In the same way as letters consist of content and envelope, data packets consist of so-called payload and header. When data packets arrive on their way through computer networks on an intermediary node (a router or a switch), upon evaluating the packet's header the intermediary node will decide where and how it will forward the packet to. It will, however, not evaluate the packet's payload. If it nonetheless does, this activity is called Deep Packet Inspection (DPI). DPI is thus used for packet filtering based on data packet payload.
Cookie-syncing	Cookie-syncing allows the cookie-based tracking of user IDs across several systems or machines.
Lemons Market	A term coined by Akerlof (1970) describing a market with asymmetric information between buyer and seller regarding the quality of goods and services. According to Akerlof, buyers use statistical methods to judge the quality of goods and services and adjust their willingness to pay to a lower level. This in turn raises the incentive of sellers to supply poor quality goods and services, since the expected return for good quality goods is relatively low. Ultimately, this process leads to a reduction of the average quality of goods and services in the market.
Browse-wrap contract	A contract or license agreement where the user agrees with the terms and conditions of the downloadable product without an explicit manifestation of asset.

Opportunity Costs	Opportunity costs refer to costs incurred by missed opportunities. They represent the loss of utility that emerges when choosing a particular action in respect of an alternative one.
Tor Browser	The Tor Browser enables Internet users to benefit from the software project that was originally called “The Onion Router”. The software is free and redirects Internet traffic through a free, worldwide, volunteer network consisting of more than 6,000 relays to conceal a user’s location and usage from anyone conducting network surveillance or traffic analysis.
Transaction Costs	Costs arise in market exchange other than the market price of the exchanged good or service.

Imprint

WIK-Consult GmbH
Rhöndorfer Str. 68
53604 Bad Honnef
Germany
Phone: +49 2224 9225-0
Fax: +49 2224 9225-63
eMail: info(at)wik-consult.com
www.wik-consult.com

Person authorised to sign on behalf of the organisation

General Manager	Dr. Iris Henseler-Unger
Head of Department Postal Services, Logistics, and Transport	Alex Kalevi Dieke
Director	J. Scott Marcus
Director	Dr. Ulrich Stumpf
Head of Administration	Karl-Hubert Strüver
Chairman of the Supervisory Board	Winfried Ulmen
Registered at	Amtsgericht Siegburg, HRB 7043
Tax No.	222/5751/0926
VAT-ID	DE 123 383 795