International Journal of Information Systems and Project Management

Volume 7 | Number 3 Article 3

2019

Consumer perspectives on information privacy following the implementation of the GDPR

Wanda Presthus
Kristiania University College

Hanne Sørum
Kristiania University College

International Journal of
Information Systems and Project Management
ISSN (print):2182-7796, ISSN (online):2182-7788, ISSN (cd-rom):2182-780X
Available online at www.sciencesphere.org/ijispm

Consumer perspectives on information privacy following the implementation of the GDPR

Wanda Presthus
Kristiania University College, Department of Technology
Christian Krohgs gate 32, 0186 Oslo
Norway
wanda.presthus@kristiania.no

Hanne Sørum
Kristiania University College, Department of Technology
Christian Krohgs gate 32, 0186 Oslo
Norway
hanne.sorum@kristiania.no

Abstract:
The General Data Protection Regulation (GDPR) was implemented in the European Union and European Economic Area in May 2018. The GDPR aims to strengthen consumers' rights to data privacy in the wake of technological developments like big data and artificial intelligence. This was a hot topic for stakeholders, such as lawyers, companies and consumers, prior to the GDPR's implementation. This paper investigates to what extent consumers are concerned about information privacy issues following the implementation of the GDPR. We present findings from an online survey conducted during spring 2019 among 327 Norwegian consumers, as well as findings from a survey conducted immediately prior to the implementation of the GDPR in spring 2018. We draw the following conclusions: (1) consumers gained significant knowledge about their information privacy from the GDPR, but felt relatively little need to execute their enhanced rights; (2) about 50% of respondents believed themselves to have control over their data, while almost 40% stated that they had no control about their personal data; and (3) consumers largely trusted companies to manage their personal data. These insights are of interest to both academia and to industries that deal with personal data.

Keywords:
information privacy; General Data Protection Regulation; GDPR; consumers; online survey.

DOI: 10.12821/ijispm070302

Manuscript received: 29 March 2019
Manuscript accepted: 22 May 2019

1. Introduction

The aim of this paper is to study information privacy from a consumer perspective following the European Union's (EU's) implementation of the General Data Protection Regulation (GDPR). Information privacy has sparked academic interest since Warren and Brandeis's seminal paper in 1890, which defined 'privacy' as 'the right to be left alone' [1 p. 994]. Numerous studies since then have investigated privacy, as well as the subcategory 'information privacy', which focuses on an individual's control over their personal data. Overall, these studies have produced a number of frameworks, models and taxonomies, such as the PAPA framework [2], the privacy calculus model [3] and Solove's taxonomy of privacy [4]. Research has also shown that consumers do not seem to be particularly concerned about their privacy [5, 6] and that the reasons for this vary, from lack of consumer understanding of the concept [4], to a conscious, calculated decision to give up personal data in exchange for benefits [3] to confusion or resignation [7]. *"In 1999, the CEO of Sun Microsystems® proclaimed that 'You have zero privacy anyway…get over it'*. More recently, Mark Zuckerberg of Facebook similarly declared that *'The age of privacy is over.'* [7 p. 64]. However, others clearly advise individuals to protect their privacy and not to surrender it without notice or choice: *'We can and must resist'* [7]. Against this background, consumers gained legal protections for their information privacy when the GDPR was implemented on May 25th, 2018.

While the GDPR is at heart a legal policy, it also affects other fields, such as information systems. For example, companies must comply with the GDPR by securing customer data, informing visitors to their websites about their rights and altering their information systems so that customers can understand, change or even delete certain personal data [8, 9]. A company's failure to comply can result in high fines and a loss of reputation. After the implementation of GDPR, Google's French operation was the first company to be sued for lack of transparency and unclear user consent conditions, when the French Data Protection Authority sued Google for 50 million Euros [10]. Similarly, the Norwegian Data Protection Authority sent the Directorate of Norwegian Customs a warning for a fine for nearly 100,000 Euros for its collection and management of customer data from surveillance cameras without appropriate consumer consent, in a case concerning 80 million records of traffic movements in which it was possible to identify the drivers' faces [11].

Shortly prior to the implementation of the GDPR, we conducted a survey (n = 216) revealing that consumers were somewhat or highly aware of the impending GDPR but were only somewhat concerned with their privacy in general [6]. The present paper follows up on those findings and seeks to discover to what extent consumers are concerned about information privacy issues following the implementation of GDPR. This paper draws on a survey (n = 327) conducted among Norwegian consumers during spring 2019, nearly a year after the implementation of the GDPR.

The rest of this paper has the following structure: first, we present related work on information privacy and the GDPR in Section 2. Then we describe our method in Section 3, followed by our results and discussion in Sections 4 and 5, respectively. Finally, we conclude in Section 6.

2. Related work on information privacy and the GDPR

In this section we present related work on information privacy in the information systems (IS) discipline (as opposed to, for example, a philosophical, psychological, marketing or legal context [12]), followed by a brief description of GDPR.

2.1 Information privacy

Our point of departure was the extensive paper by Bélanger and Crossler [12] that conducted a literature review of information privacy within an information systems context. In our digital society, IS are highly important for the development of almost any human organisation [13] and this rapid development entails both challenges and opportunities [14]. Several papers conclude that, in our digital age, trust is highly important, especially regarding online transactions and the handling of sensitive personal information [15], since, based on an analysis of an individual's transactional data, companies can now understand and predict that individual's preferences and future behaviour. Moreover, a study by Chang et al. [16] found that perceived privacy control among online banking customers

significantly affected customers' trust and perceived privacy. At the same time, however, Obar and Oeldorf-Hirsh [17] found that 74% of people signing up for a social networking service skipped reading the privacy policy, which should have taken 29–32 minutes to read through, and spent on average less than 1 minute reading the terms of service, which should have taken 15–17 minutes to read through. This indicates that users pay little or no attention to such information and introduces what researchers call the privacy paradox [12], in which consumers claim to be concerned with their privacy but do not behave accordingly. For example, a consumer may express an intention to protect her personal data, yet will quickly disclose them in exchange for convenience when shopping online. According to Bélanger and Crossler [12], this is an important aspect of studying information privacy: *'Even if other streams of IS research suggest that intentions lead to behaviors, the privacy paradox should be explored further to provide an understanding as to why such is not the case with information privacy. Furthermore, researchers should not assume de facto that intentions lead to behaviors when information privacy research is conducted'* [12, p. 1021]. Similarly, another study on the privacy paradox found that consumers were willing to trade their privacy in exchange for perceived security benefits, convenience and efficacy [18]. Additional studies have also found this variant of the privacy paradox specifically among social media users, and have called it the 'privacy trade-off' [19]. At the same time, other research has called into question whether consumers really care if a retail store can use their data to predict things about them, for example pregnancy [20].

2.2 The GDPR

The GDPR went into effect on May 25th, 2018 in all EU and European Economic Area (EEA) countries. Technological advances like big data and artificial intelligence have made personal data abundant and ubiquitous, and it is now easy for companies to collect and analyse online consumers' behaviours and shopping habits. The aim of the GDPR is therefore to *'harmonize data privacy laws across Europe'* (https://gdpr-info.eu/) and to increase consumer rights and transparency [9]. Its 99 articles can be found in full online. The first article states that *'This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data'*; in other words, consumers have enforceable rights to their personal data. Article 4 further states that *'"personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier…'*.

Prior to its implementation, the GDPR and privacy rights were hot topics of discussion in Norway and many companies sought to implement the requirements of the GDPR. While it is interesting to understand how the regulation affects individuals, it is also vital that companies understand and implement the GDPR's privacy requirements, and publications have sought to guide companies and provide them with practical advice and solutions [9]. Although a study on GDPR compliance in Norwegian companies found that most companies were well informed about the new regulations and rated themselves as well prepared, many were interested in addressing practical issues and challenges introduced by the regulations [8]. It seems likely that the French lawsuit against Google will be only the first of many prosecutions brought against companies for violating the GDPR. Moreover, the implementation of the GDPR presents a number of technological challenges as well as solutions. For example, a consumer may request the deletion of their data, but this may prove technologically impossible despite a company's best efforts at compliance [21, 22]. The French case against Google also illustrates how far the GDPR reaches: it affects any company that interacts with citizens of the EU or EEA, meaning that even American-based companies like Google and Facebook must follow the GDPR if they have users from the EU or EEA [23]. However, GDPR does not come without challenges. Koops has critically pointed to technological challenges as well as changing the mindset of developers [21, 22], and Mateosian has challenged the consumer with asking whether it really matters if a retail store can predict pregnancy [20]. It remains to be seen exactly what difficulties may arise from this new regulation.

In the present study, we focused on seven aspects of the GDPR, see Table 1. We selected these topics based on two criteria: first, they were emphasised by the Norwegian Data Protection Authority (https://www.datatilsynet.no/rettigheter-og-plikter/den-registrertes-rettigheter/) and by Jarbekk and Sommerfeldt [9], and second, they are specifically directed towards consumers (as opposed to organisations, for example Article 37 of the GDPR, *'Designation of the data protection officer'*).

Table 1. Our seven topics and corresponding GDPR articles

Topic	Article(s)	Notes
Right to information	5, 12, 13, 14	The individual has the right to know how companies collect and store personal data.
Right to access, change or restrict the processing of information	15, 16, 18	Consumer questions or requests for their personal data must be answered within 30 days. During this period, their data can be stored by the company but not processed.
Right to erasure	17	Right to have parts of their personal data deleted.
Right to data portability	20	Right to transfer personal data.
Right to object	21, 30, 7	Consumers must be given the chance to approve a company's online terms and conditions, acceptance of cookies and marketing.
Automated individual decision making	22	Consumers must be notified of the use of artificial intelligence and automated decision making.
Territorial scope, trade for benefits	3	Facebook, disclosing data for benefits.

3. Methods

Our data were collected during February and March 2019 via an online survey questionnaire that was developed with the software tool SurveyMonkey®. The questionnaire consisted of 17 questions, including 4 background questions, 12 primary survey questions or statements and 1 open comment field at the end of the survey (see Appendix). Respondents could also provide qualitative feedback for all of the 12 primary survey questions. The purpose of the survey was to generate insights into consumer views about information privacy and to give respondents an opportunity to share their reflections and thoughts related to the survey topics. The questionnaire included Likert-scale, multiple-choice and open-ended questions that requested qualitative answers. The questions also drew inspiration from a prior survey that we conducted in 2018 [6]. A progress bar was visible at the bottom of each survey page so that respondents could see how much work remained to complete the survey.

The survey respondents were first shown an introductory text at the beginning of the questionnaire that informed them about the survey contents. Participation was voluntary and anonymous, and participants could quit the survey at any time. The data were collected through a weblink created by SurveyMonkey®. Before the survey launched, we conducted a pilot test with three respondents and both the desktop and mobile versions of the questionnaire; the pilot test participants were not members of the research team. The pilot test resulted in a few modifications and changes to the survey: some questions were reworded for clarity and some additional answer options were included.

The final survey received 327 respondents before being closed to further participation. Since not everyone who started the survey completed it, our results report the number of respondents (*n*) for each of the findings reported in this paper. The average time to complete the survey was 6 minutes. The research team carefully reviewed and discussed all of the answers and used descriptive statistics to get an overall impression of the data. We also selected some particularly relevant questions from the survey for more detailed analysis.

3.1 Respondent profiles

Table 2 provides an overview of the survey respondents. More men (54%) participated than women (45%). Most respondents were 21–25 years old, followed by the 26–30-year-old group. The data also show that 62% of respondents had heard of the GDPR and stated that they understood the meaning of the term and the content of the regulation; 31% knew a little bit; 3% had a vague understanding and almost 5% had never heard of the GDPR.

Table 2. Respondent characteristics in percentage, with the actual number of respondents in parentheses

Characteristic	Measurement scale
Gender	Female: 44.65% (146); male: 54.43% (178); did not specify: 0.92% (3).
Age (years)	Under 18: 0% (0); 18–20: 7.03% (23); 21–25: 56.27% (184); 26–30: 17.74% (58); 31–35: 7.34% (24); 36–40: 3.98% (13); 41–50: 6.12% (20); 51–60: 0.92% (3); over 60: 0% (0); did not specify: 0.61% (2).
Occupational status	Employed: 19.27% (63); student: 80.73% (264).
Knowledge of the GDPR	'Yes, and I know what it means': 61.77% (202); 'Yes, I know a little, but not enough about what it means': 30.58% (100); 'Yes, but I do not know what it means': 3.06% (10); 'I have never heard of that': 4.59% (15).

4. Results

Section 4.1. presents the results from the survey conducted in spring 2019, following the implementation of the GDPR. Section 4.2 contains some comparison highlights from a previous study we conducted immediately prior to the implementation of GDPR in early 2018 [6].

4.1 Main results from the spring 2019 survey

Table 3 shows participants' general thoughts on information privacy. The findings are structured according to three categories: control over personal information ('control'), awareness of the new regulation ('awareness') and opinions of their enhanced rights ('enhanced rights').

Table 3. General thoughts on privacy and the GDPR

Key word	Question	Answer alternatives
Control (n = 327)	To what extent do you find that your personal information exists in places that you do not have control over? (E.g., information stored in databases of different businesses)	I have control over everything: 0.92% (3) I have a lot of control: 8.87% (29) I have partial control: 46.79% (153) I have no control at all: 38.53% (126) I do not care about it: 4.89% (16)
Awareness (n = 327)	On July 20, 2018, the GDPR (General Data Protection Regulation) was introduced in Norway. Have you heard about it? (before you started answering this survey)	Yes, and I know what that means: 61.77% (202) Yes, I know a little, but not enough about what it means: 30.58% (100) Yes, but I didn't know what that meant: 3.06% (10) I had never heard of that: 4.59% (15)
Enhanced rights (n = 327)	The GDPR means that individuals have gained new rights regarding the collection and storage of personal data. What do you think about that?	I think my rights have improved: 59.81% (192) I don't think my rights have improved: 19.63% (63) I don't care at all: 3.74% (12) Do not know: 16.82% (54)

We then asked respondents to go into more detail about their enhanced rights; these results are shown in Table 4.

Table 4. Enhanced data rights under the GDPR

		Answer alternatives				
Key word	**Statement/question**	I have executed this right	I might execute this right	I will most likely not execute this right	I do not care	I do not know
Access and rectification (*n* = 321)	The GDPR gives you the right to receive a reply within 30 days when you approach businesses with questions related to your data. The overview should be sent in a readable format and you can correct any errors. What do you think about this?	7.17% (23)	59.81% (192)	22.74% (73)	2.18% (7)	8.10% (26)
Erasure (*n* = 321)	The GDPR has given you a greater right to demand that some personal information (that companies have collected) about you will be deleted. What do you think about this?	14.95% (48)	66.98% (215)	12.77% (41)	1.56% (5)	3.74% (12)
Objection (*n* = 327)	You have the right to object to companies sending you direct marketing (in the form of personal customised advertising).	32.11% (105)	36.09% (118)	22.32% (73)	3.67% (12)	5.81% (19)
Data portability (*n* = 321)	Data portability is a key part of the GDPR. This means that you can transfer all your data that one business has saved. You can require existing business to send your data to, for example, a competitor business. What do you think about this?	6.54% (21)	40.81% (131)	36.45% (117)	4.36 % (14)	11.84% (38)

Table 5 displays our findings regarding transparency, territorial scope and trade for benefits.

Table 5. Transparency, territorial scope and trade for benefits

Key word	**Question**	**Answer alternatives**
Cookies (*n* = 321)	The GDPR says that you can choose to accept some cookies, but not all, when you visit a website. In addition, the purpose of the data stored about you should be more disclosed. What do you think about this? (Check all appropriate options)	Companies have become much better at informing website visitors about cookies: 46.73% (150) Companies allow me to opt out of some cookies: 21.18% (68) I am unsure what companies actually do when it comes to cookies: 27.10% (87) I do not care: 4.67% (15) Do not know what cookies are: 0.31% (1)
Terms and conditions (*n* = 314)	When you download an app on your cell phone or install a programme on your laptop, you must approve the terms and condition. What is your typical reaction?	I read the whole text, even though it takes a long time: 0.96% (3) I quickly scroll through the entire text, but do not read everything: 16.56% (52) I click on "I agree/accept" without looking at the text at all: 62.10% (195) It depends on how much time I have or depends on the app/programme in question: It depends from time to time (depending on the app/programme in question: 20.38% (64)
Artificial Intelligence (*n* = 315)	Artificial intelligence makes it increasingly possible for companies to make automated decisions without the involvement of a human. I think it's okay that a machine algorithm performs and calculates the following: (check all appropriate options)	Whether or not I get a mortgage: 27.30% (86) The price of my insurance: 49.52% (156) How much I will receive in student loans: 49.52% (156) My examination assessments and determinations of my grades at school: 13.97% (44) What movies I should watch on Netflix (or similar services): 83.49% (263) What products have been purchased by others who also bought an item I bought on Amazon (or similar online store): 72.70% (229) Whether I am entitled to compensation if I am stripped of an asset: 24.76% (78)
Facebook, trade-off (*n* = 313)	The GDPR also affects companies outside the EU/EEA. What do you think about Facebook being affected in the ways mentioned in the other questions (for example, the right to access, rectification and deletion of data)?	I think it is great that Facebook is affected by the GDPR: 85.30% (267) I find it unfortunate that Facebook is affected by the GDPR: 2.88% (9) I do not care at all: 3.83% (12) I do not know: 7.99% (25)

4.2 Main results from the of pre-GDPR survey

We conducted a similar survey (n = 216) in early 2018, right before the implementation of the GDPR [6]. The questions differed somewhat from the post-implementation survey since we addressed comments from some participants of the first survey—namely, that they wanted a more in-depth survey and that some of our answer options were too leading. Table 6 shows the main findings from this survey.

Table 6. Main findings from the pre-GDPR survey [6]

Key word	Question	Selected answer options
Knowledge of GDPR	Have you heard about the GDPR?	Yes, and I know what it means: 46.76% (101); Yes, I know a little, but not enough about what it means: 26.39% (57)
Attitude	Implementation of the GDPR means that your information privacy rights will be enforced. What do you think about that?	It sounds very good: 64.04% (130); It sounds very good, but I do not think that it will make any difference for me as consumer: 31.03% (63)
Enhanced rights	Data portability Erasure Insight (within 30 days from companies) Agree to some cookies, but not all Terms and conditions	This is something I might execute: 53.20% (108) This is something I might execute: 48.28% (98) This is something I might execute: 52.22% (106) It sounds very good: 63.05% (128) I click on "I agree/accept" without looking at the text at all: 70.98 (137)
Artificial intelligence	I think it is acceptable that an algorithm automatically decides:	Which movies I should watch on Netflix: 80.41% (156)
Territorial scope	What are your thoughts about Facebook being affected by the GDPR?	I really hope so, because Facebook has no respect for privacy: 69.09% (114)
Trade for benefits	Which data are you willing to give up in exchange for better services or discounts?	Top three: First name: 92.02% (173); family name: 75.00% (141); e-mail address: 88.30% (166)

Overall, we found that (1) most consumers were moderately or very aware of the GDPR and of their rights in this regard but that they were sceptical of how the new regulations would be handled by organisations; (2) there were variations among the consumers in how they perceived the collection and storage of personal data, depending on the nature of the data in question; and (3) the consumers indicated relatively high concern for their privacy.

5. Discussion

In this section we discuss our findings against existing research as presented in section 2. We have arranged the discussion according to the seven topics as presented in Table 1.

5.1 Right to information

Our findings from our post-GDPR survey indicate that 56% of respondents had a moderate interest in information privacy, while 31% indicated a stronger interest; this suggests that most consumers care about this topic. These results are nearly the same as those from the survey conducted shortly prior to implementation of the GDPR [6].

We received 30 comments about this question on the post-GDPR survey, many of them thorough. These indicated a variety of responses, ranging from anxiety about information privacy to feelings of trust and not feeling threatened. Some prior research has argued that consumers lack an understanding of privacy as a concept and what it comprises; consumers are quick to exclaim *'This violates my privacy'* ([4] p. 480) and leave it at that. Addressing this problem, Solove created a taxonomy with four categories: (1) information collection, (2) information processing, (3) information dissemination, and (4) invasion. Each of these contains harmful activities such as surveillance, identification, blackmail, decisional interference and more. We agree that the average consumer lacks knowledge about technological advances. There are many algorithms and technologies at play when a consumer goes into a store or browses the Internet, including surveillance cameras, the ability to trace an individual through their smartphone, websites that harvest cookies

and web beacons [24]. Most of our participants were relatively young (56% were between 21 and 25 years old) and relatively well educated (76% held a bachelor's degree), and should therefore be accustomed to using smartphones, the Internet and other advanced technology; yet they did not seem to reflect much about their potential risks. A few responses, however, suggested that consumer interest in these topics may be increasing: *'Maybe I have too much trust'* and *'My concern is medium, but it is INCREASING'*. Unfortunately, our survey could not determine whether such changes in awareness or concern were due to the implementation of the GDPR.

5.2 Rights to access, rectify and restrict the processing of personal information

The GDPR ensures that consumers have the right to view a copy of their personal information that a company has collected and stored. Although very few of our respondents indicated that they had availed themselves of this new option, 60% said that they might do so in the future, and only 23% said that they did not expect to. This suggests that consumers are somewhat concerned about what data are being stored and that they want at least some control over access to their personal data. Among the eight comments we received on this topic, three specifically mentioned Facebook: *'Have done this with Facebook—meaning downloading the data they have about me—or, at least what they want me to think they have'*; *'Scary to read what Facebook knows about me—even stuff I have deleted earlier'*; and *'Have downloaded my data from Facebook for two reasons: backup, and to see what they look like'*. Another participant claimed that several companies did not comply within 30 days. The importance of consumer access is thoroughly addressed in Mason's PAPA framework [2]. Mason describes one case where a bank customer was wrongfully accused of not paying back his house loan. This was in the mid-1980s and the customer had proof of payment in the form of a booklet with a stamp, but the bank refused this evidence and said that it was not registered in the IT system. When the customer finally got enough resources to sue the bank his wife had suffered as stroke due to stress. The family got a settlement in cash, but no excuse. The GDPR now allows consumers in the EU/EAA to see what information of theirs is being recorded and stored and gives these consumers a right to rectify errors; however, none of our participants said that they had made any rectifications.

5.3 Right to erasure ('right to be forgotten')

Under the GDPR, consumers also have the right to have some of their personal data deleted. This applies to information that companies have collected and stored about an individual—although it is also important to note that the GDPR does not include a right to have *all* one's data deleted, only select portions of it. For example, if a customer chooses to pay with a credit card, the record of this transaction and associated data cannot be deleted.

Among our respondents, 68% believed that they might want to ask a company to delete their data and 15% had already done so. This provides further evidence that privacy issues concern many consumers. How organisations will enact such requests in practice remains of interest, as it will require additional work. In many companies, it can require changes in routines, data systems and resource prioritisation. The six comments that we received on this topic mostly expressed some scepticism. Reasons for their scepticism included a lack of information on how to erase their data and statements such as *'I no longer know which companies possess data about me'*. One participant stated that they planned to delete their personal data on Google and Facebook once they figured out how. However, another comment stated that *'I will most likely not pursue this. From the advertisements that Facebook continuously shows me, I draw the conclusion that they do not really know too much about me as a person'*.

Respondents' concerns on this topic are understandable: how can we, as consumers, really know if an organisation has indeed deleted all our personal data? Respondents expressed scepticism regarding both the organisations' *will* to delete information as well as their *capacity* to do so. (However, we must remember that GDPR does not give us the right to have all data deleted. As previously stated: if a customer chooses to pay with credit card this transaction data cannot be deleted). Extant literature has repeatedly highlighted this issue, and some have claimed that it is impossible for companies to fully comply with the GDPR regarding 'the right to be forgotten' [21]. We asked the Norwegian Data Protection Regulation office for advice on how an individual can assure deletion; they responded that a consumer has to trust the organisation, although they can also pay attention to the marketing that they receive from that organisation

afterwards. Also, a consumer can execute their right to data portability to later check if the data in question are in fact deleted, as we discuss in the next section.

5.4 Right to data portability

Data portability is a key part of the GDPR and means that consumers can ask a business to transfer all of their personal data to a competing company, thus giving consumers greater control over their personal information and making it easier for consumers to switch from one company to another. Our survey results indicated that respondents held somewhat mixed views on this topic: 41% stated that they might take advantage of this and 36% stated that they probably would not (12% were uncertain). Only 7% had previously attempted this. We received 13 comments on this question. Notably, 3 specifically stated that they had asked Facebook to send them all their accumulated data, but they did not elaborate further. Facebook has indeed made it possible for consumers to access this right, as illustrated in Figure 1 below. A Facebook user can monitor his or her information in five ways: access the information; download (thus facilitating the rights of data portability); view the activity; managing the information; and deleting their profile. Assessing how well Facebook fulfils these five rights is beyond the scope of this study.

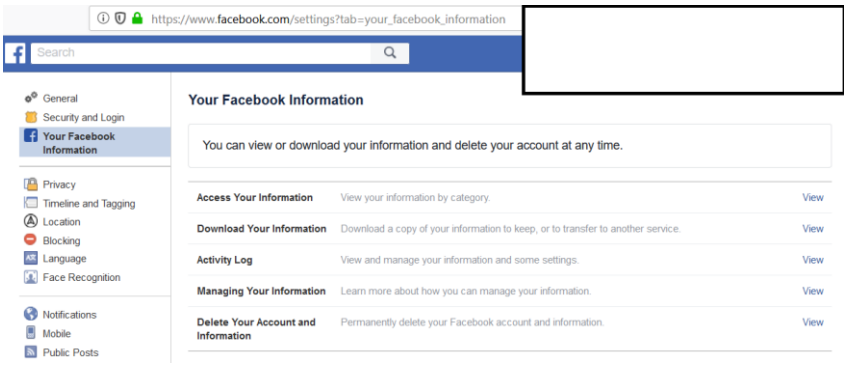

Fig. 1. Screenshot of Facebook's information privacy features for users

On the one hand, we observe that consumers are somewhat carefree when it comes to their personal data [6], but on the other hand, it seems that consumers place a high price on it. For example, David Jacoby, an international security analytic, said that his friends assessed their Facebook-account to be worth approximately 50.000 Euro [25]. However, the price on the dark web is about 1 Euro and this also illustrates the mismatch between the users' perceptive and the hackers in general. It may also illustrate the privacy paradox which we return to in Section 5.7.

Other comments came from respondents who indicated that they might execute this right of data portability in the future: '*This is a good initiative. For example, if I want to change opticians, I can easily ask them to transfer my information to another optician's shop, meaning that I will not have to undergo new visual examinations.'* However, other respondents expressed some concern about how this will be handled by companies.

5.5 Right to object

Although consumers have the right to object to a website or application's 'terms and conditions', our results indicate that consumers were very quick to approve them even though it was quite clear that they were not very familiar with the content; without reading it, they trusted that it was acceptable. Only 1% of our respondents stated that they took the time to read the entire text, while 17% scrolled through quickly and did not read everything. Over 60% clicked on 'accept' without reading the text at all (the remaining 20% reported that their reactions vary). Even though most of our respondents stated that they cared about privacy, the majority were unlikely to spend time reading the terms and conditions of a programme they were downloading. We received nine comments on this topic, most expressing the view that such texts were too long or too difficult to understand.

The GDPR also allows consumers to choose to accept some but not all website cookies when visiting a website. Companies should therefore disclose the purpose of the personal data stored by each cookie. Since the GDPR came into force many companies have implemented this feature and visitors to a website now often encounter pop-up information boxes describing the website's cookie use. Almost half of our respondents felt that companies have become much better at informing website visitors about cookies since the implementation of the GDPR. Just under 30% stated that they felt uncertain about what companies do with cookies, and just over 20% claimed that companies give consumers the opportunity to opt out of some cookies. This topic also seemed to be of interest to our respondents, as 23 chose to leave additional comments. These comments indicated three main areas of concern: (i) the pop-up boxes with cookie information are more irritating and annoying than before GDPR, (ii) it is not possible to choose to accept only some cookies and (iii) the option to deny cookies was irrelevant, since *'you cannot have any websites without cookies anyway'* and *'it is not really the cookies that pose a threat to my information privacy'*.

The GDPR also gives consumers the right to object to direct marketing (such as personalised advertising). We found that attitudes towards this topic were fairly mixed: 32% of our respondents had made use of this ability, while 36% said that they might do so in future and 22% said that they most likely will not. The 24 comments we received on this topic were on the whole more positive than the comments we received about cookies. In general, they expressed happiness about the ability to opt out of receiving newsletters and personalised recommendations. However, some comments pointed to the fact that marketing is necessary. Other comments stated that *'I would rather get personal recommendations than generic commercials*' and *'If my personal data are only used to present me with direct marketing, I see no problem'*.

User consent to terms and conditions, the use of cookies and direct marketing can be a double-edged sword. For example, to a greater extent than before the implementation of GDPR, consumers have now become accustomed to approving the use of website cookies. However, so long as consumers do not bother to read the text, this can function as a trap [26]. In other words, although consumers have now become accustomed to clicking on statements such as 'I understand that this website uses cookies', we suspect that the average consumer does not always understand what cookies really are and their potential consequences, even though very few of our respondents admitted to not knowing what cookies are (3 respondents in the pre-GDPR study and 1 participant in the post-GDPR study). However, it is one thing to know what cookies are and another to fully understand how they can be (mis)used. 27% (87) participants agreed with the statement *'I am unsure what the companies are doing regarding cookies'*. Cookies typically include login information, user preferences and/or online shopping cart information. In addition, third-party cookies communicate collected data to advertisers and flash cookies can continue to collect and track a user's data even after a user has deleted their cookies [27]. Moreover, the new and overwhelming use of pop-up boxes stating that 'this website uses cookies' may lead companies to feel that this justifies their abuses of consumers' personal data.

5.6 Automated, individual decision making

The increasingly widespread usages of algorithms, artificial intelligence and big data (such as high-volume, high-speed and highly heterogeneous data) were drivers for the development of the GDPR [9, 28]. The GDPR does not forbid the use of such technologies, but calls for greater transparency about their use. These technological advances make human participation redundant in a continually increasing percentage of decisions, such as whether an individual qualifies for a mortgage loan, whether an immigrant should be granted citizenship or how long a convict should be sentenced to prison. In schools, multiple-choice exams have long been used to calculate student grades, but it is now also possible to for algorithms to grade unstructured essays without the involvement of a human instructor [6].

A large majority of our respondents were happy to receive personalised suggestions on Netflix or similar services (83%) or for other products that might be of interest to them, for example on Amazon (73%). Half of our respondents also felt that it was acceptable to use artificial intelligence in connection with insurance and student loan decisions. However, less than 30% of respondents were comfortable with the use of artificial intelligence to determine consumer eligibility for mortgage loans, and only about 25% of respondents believed that it should be used to decide whether an individual was entitled to compensation after being robbed. Moreover, only about 15% of respondents agreed that artificial

intelligence should assess exam results. The 21 comments that we received on the topic of automated decision making were largely in agreement with each other and reflected the results noted above. Regarding critical decisions such as mortgage and student loan eligibility, the comments indicated an acceptance of algorithms being used as a component of the decision making process, but felt that a human should be involved in the final decision. They also very clearly indicated a desire for transparency about the use of automated decision making and a belief that consumers should have the right to appeal automated decisions. Consistent with our previous study [6], we found that the use of algorithms and artificial intelligence was more accepted in decisions with fewer consequences, such as movie recommendations. It is nonetheless noteworthy that as many as 15% accepted the use of artificial intelligence in assessing exams, and it will be interesting to follow technological and societal evolutions on this topic [29].

5.7 Territorial scope, trade for benefits

Almost everyone who participated in our survey said they were willing to disclose their first name (90%) on websites and most were also willing to disclose their last name (74%), in order to receive perceived benefits. Most were also willing to leave an e-mail address (80%) and roughly half of respondents were also willing to provide their date of birth and to list the kinds of products they purchased and what kinds of television they watched. However, few people wanted to divulge their iris patterns, fingerprints or bank card numbers; these are highly personal data that consumers wanted to keep private. Interestingly, although we only received five comments on this topic, all of them expressed satisfaction with Facebook, in particular, being affected by the GDPR. One comment stated that *'I have a love/hate relationship with Facebook. I have no doubts that they have sold my personal data'*. We also asked respondents about their willingness to trade their personal data for perceived benefits, such as corporate discounts or improved services. The 12 comments that we received on this topic primarily referred to two issues: the amount of trust a consumer placed in a given company and the fact that people tend to say one thing and yet do another (often referred to as the privacy paradox) [12].

5.8 Final comments

Finally, at the end of the survey we allowed respondents to leave any comments about the survey itself. Of the eight comments we received here, half were positive and called the survey interesting or eye-opening, while three stated that it was cumbersome and that the questions took too long to read. We found the final comment intriguing: *'I am personally against the whole GDPR. "The right to be forgotten" is incompatible with the very existence of the Internet. […] The future is a decentralized internet, with blockchain technology and immutable data. The GDPR is an infringement of the private sphere […] and people should react accordingly.'* We certainly agree that the GDPR is not a silver bullet that will solve all challenges to information privacy, and Section 5.5 points to some evidence of the GDPR working against its intended purpose. However, the GDPR has also initiated a useful discussion on the tangible implications of information privacy, to which we hope our present discussion of selected topics can meaningfully contribute.

Overall, our findings largely confirm prior research, especially regarding the privacy paradox. We found that consumers possess a high degree of knowledge about their rights and the GDPR; however, they typically stated that they *might* execute their rights, and only 5–30% (depending on the specific topic) actually *had* executed their rights. Although consumers are now better informed, few have taken any action to take advantage of their increased rights.

5.9 Limitations and suggestions for future research

This study was mainly descriptive and offered insights from a consumer perspective. The GDPR is a new regulation that affects any organisation dealing with personal data and consumers in the EU and EEA. Currently, our knowledge is still limited regarding how it will influence various stakeholders. The aim of this study was therefore to establish a foundation one year after its implementation. We hope that future research will build on our findings, and we suggest in-depth qualitative interviews with consumers and case studies about how companies can meet the new consumer data requirements. Although our findings indicate that consumers are only somewhat likely to execute their new rights to

information privacy, this may change over time as dynamics evolve between technologies, policies, processes, society and the economy [13, 28]. This topic remains of interest to the field of information systems and project management.

6. Conclusion

Our research responds to prior calls for more insights regarding what consumers actually think and how they act. Based on two surveys conducted prior to (n = 216) and following (n = 327) the implementation of the GDPR, we offer three main insights. (1) Within a year, consumers gained increased knowledge about their information privacy; however, they remained fairly unconcerned about executing their enhanced rights. (2) Beliefs about personal control of one's own data were highly mixed: about 50% of respondents felt that they had control of their personal data, while almost 40% stated that they had no control over their personal data. (3) A recurring issue was consumers' trust in companies' management of their personal data. The present research can contribute to the field's understanding of consumer views of information privacy and the GDPR. While the GDPR is not likely to solve all problems pertaining to information privacy, it remains an interesting and relevant subject for future research.

Acknowledgements

We thank the anonymous survey participants and everybody who helped with our data collection. We also thank the reviewers of the International Journal of Information Systems and Project Management (IJISPM) who helped improve the quality of our paper. Finally, this paper builds on and extends our research based on a survey conducted prior to the implementation of the GDPR [6], and we are grateful for the reviews of that study.

References

[1] H.J. Smith, T. Dinev and H. Xu, "Information Privacy Research: An Interdisciplinary Review," MIS Quarterly, vol. 35, no. 4, pp. 989-1015, 2011.

[2] R.O. Mason, "Four ethical issues of the information age," MIS Quarterly, vol. 10, no. 1, pp. 5-12, 1986.

[3] T. Dinev, H. Xu, J.H. Smith and P. Hart, "Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts," European Journal of Information Systems, 22(3): pp. 295-316, 2013.

[4] D.J. Solove, "A taxonomy of privacy," University of Pennsylvania Law Review, 154, pp. 477-560, 2005.

[5] J.L. Zittrain, "The Future of the Internet - and How to Stop it," Yale University Press, 2008.

[6] W. Presthus and H. Sørum, "Are Consumers Concerned About Privacy? An Online Survey Emphasizing General Data Protection Regulation," Procedia Computer Science, 138, pp. 603–611, 2018.

[7] S. Few, "Big Data, Big Dupe. A little book about a big bunch of nonsense," Analytic Press, 2018.

[8] W. Presthus, H. Sørum and L.R. Andersen, "GDPR compliance in Norwegian Companies," Norsk konferanse for organisasjoners bruk av IT (NOKOBIT). Svalbard, Norway, 2018, pp.1-14.

[9] E. Jarbekk and S. Sommerfeldt, "Personvern og GDPR i praksis," Cappelen Damm, 2019.

[10] NTB. (January 21st, 2019) Fransk gigantbot til Google. Nettavisen. [Online] Available: https://www.nettavisen.no/nyheter/utenriks/fransk-gigantbot-til-google/3423583247.html 2019.

[11] J.S. Dahl (March 12th, 2019) Varsel om gebyr til Tolldirektoratet [Norwegian]. Datatilsynet [Online] Available: https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-20192/varsel-om-gebyr-til-tolldirektoratet

[12]F. Bélanger and R.E. Crossler, "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," MIS Quarterly, vol. 35, no. 4, pp. 1017-1041, 2011.

[13] J. Varajão, "The many facets of information systems (+ projects) success," International Journal of Information Systems and Project Management, vol. 6, no. 4, pp. 5-13, 2018.

[14] J. Kaidalova, K. Sandkuhl and U. Seigerroth, "How Digital Transformation affects Enterprise Architecture Management–a case study," International Journal of Information Systems and Project Management, vol. 6, no. 3, pp. 5-18, 2018.

[15] G. Bansal, F.M. Zahedi and D. Gefen, "Do context and personality matter? Trust and privacy concerns in disclosing private information online," Information & Management, vol. 53, no. 1, p. 1-21, 2016.

[16] Y. Chang, S.F. Wong, C.F. Libaque-Saenz and H. Lee, "The role of privacy policy on consumers' perceived privacy," Government Information Quarterly, vol. 35, no. 3, pp. 445-459, 2018.

[17] J.A. Obar and A. Oeldorf-Hirsch, "The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services," Information, Communication & Society, pp. 1-20, 2018:

[18] R.E. Crossler and C. Posey, "Robbing Peter to pay Paul: Surrendering privacy for security's sake in an identity ecosystem," Journal of the Association for Information Systems, vol. 18, no. 7, pp. 487-515, 2017.

[19] D. O'Brien and A.M. Torres, "Social networking and online privacy: Facebook users' perception," Irish Journal Of Management, vol. 31, no. 2, pp. 63-97, 2012.

[20] R. Mateosian, "Ethics of Big Data," IEEE Computer Society, vol. 33, no. 2, pp. 61–62, 2013.

[21] B.-J. Koops, "Forgetting footprints, shunning shadows: A critical analysis of the right to be forgotten in big data practice," SCRIPTed, 8: pp. 229-256, 2011.

[22] B.-J. Koops and R. Leenes, "Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design'provision in data-protection law," International Review of Law, Computers & Technology, vol. 28, no. 2, pp. 159-171, 2014.

[23] K.E. Martin, "Ethical issues in the big data industry," MIS Quarterly Executive, vol. 14, no. 2, pp. 67-85, 2015.

[24] W. Presthus and L. Andersen, "Information Privacy from a Retail Management Perspective," Proceedings of the 25th European Conference on Information Systems (ECIS), Guimarães, Portugal, pp. 1968-1983. June, 2017.

[25] H.F. Høydal (March 16th, 2019.), Prisen på ditt digitale liv [Norwegian], in VG Helg. 2019.

[26] T.P. Krokfjord, T.H. Ueland and L.E. Bones (March 16th, 2019.), Slik selger de norske pesonopplysninger [Norwegian], in Dagladet, 2019.

[27] H.R. Lozada, G.H. Kritz and A. Mintu-Wimsatt, "The Challenge of Online Privacy to Global Marketers," Journal of Marketing Development and Competiveness, vol. 7, no. 1, pp. 54 – 62, 2013.

[28] P.B. Lowry, T. Dinev and R. Willison, "Why security and privacy research lies at the centre of the information systems (IS) artefact: proposing a bold research agenda," European Journal of Information Systems, no. 26, pp. 546-563, 2017.

[29] T.H. Davenport, and J. Kirby, "Only humans need apply: winners and losers in the Age of smart machines," HarperCollins Publishers, 2016.

Appendix: Questionnaire

- Gender
- Age
- Main occupation
- Level of privacy concern in general

You have the right to object to companies sending you direct marketing (in the form of personal customised advertising).
[I have executed this right - I might execute this right - I will most likely not execute this right - I do not care - I do not know]

To what extent do you find that your personal information exists in places that you do not have control over? (E.g., information stored in databases of different businesses)
[I have control over everything - I have a lot of control - I have partial control - I have no control at all - I do not care about it]

On July 20, 2018, the GDPR (General Data Protection Regulation) was introduced in Norway. Have you heard about it? (before you started answering this survey)
[Yes, and I know what that means - Yes, I know a little, but not enough about what it means - Yes, but I didn't know what that meant - I had never heard of that]

The GDPR means that individuals have gained new rights regarding the collection and storage of personal data. What do you think about that?
[I think my rights have improved - I don't think my rights have improved - I don't care at all - Do not know]

Data portability is a key part of the GDPR. This means that you can transfer all your data that one business has saved. You can require existing business to send your data to, for example, a competitor business. What do you think about this?
[I have executed this right - I might execute this right - I will most likely not execute this right - I do not care - I do not know]

The GDPR has given you a greater right to demand that some personal information (that companies have collected) about you will be deleted. What do you think about this?
[I have executed this right - I might execute this right - I will most likely not execute this right - I do not care - I do not know]

The GDPR gives you the right to receive a reply within 30 days when you approach businesses with questions related to your data. The overview should be sent in a readable format and you can correct any errors. What do you think about this?
[I have executed this right - I might execute this right - I will most likely not execute this right - I do not care - I do not know]

The GDPR says that you can choose to accept some cookies, but not all, when you visit a website. In addition, the purpose of the data stored about you should be more disclosed. What do you think about this? (Check all appropriate options.)
[Companies have become much better at informing website visitors about cookies - Companies allow me to opt out of some cookies - I am unsure what companies actually do when it comes to cookies - I do not care - Do not know what cookies are]

Artificial intelligence makes it increasingly possible for companies to make automated decisions without the involvement of a human. I think it's okay that a machine algorithm performs and calculates the following: (check all appropriate options).
[Whether or not I get a mortgage - The price of my insurance - How much I will receive in student loans - My examination assessments and determinations of my grades at school - What movies I should watch on Netflix (or similar services) - What products have been purchased by others who also bought an item I bought on Amazon (or similar online store) - Whether I am entitled to compensation if I am stripped of an asset]

When you download an app on your cell phone or install a programme on your laptop, you must approve the terms and condition. What is your typical reaction?
[I read the whole text, even though it takes a long time - I quickly scroll through the entire text, but do not read everything - I click on "I agree/accept" without looking at the text at all - It depends from time to time (depending on the app/programme in question)]

The GDPR also affects citizens of countries outside the EU/EEA. What do you think about Facebook being affected in the ways mentioned in the other questions (for example, the right to access, rectification and deletion of data)?
[I think it is great that Facebook is affected by the GDPR - I find it unfortunate that Facebook is affected by the GDPR - I do not care at all - I do not know]

Which data are you willing to give up in exchange for better services or discounts?
E.g. [First name - family name - e-mail address - IP-address - fingerprint]

Biographical notes

Wanda Presthus
Wanda Presthus received her Ph.D. from Gothenburg University (Sweden) and is an Associate Professor at Kristiania University College in Oslo, Norway. Her research interests include information privacy (how companies manage personal data and how individuals react), research methods (helping junior researchers conduct their research) and business analytics (to improve decision making).

Hanne Sørum
Hanne Sørum is an Associate Professor at Kristiania University College in Oslo, Norway. She holds a Ph.D. from Copenhagen Business School (Denmark). Her research focuses on information systems, human-computer interactions, eGovernment and privacy and the GDPR. She has published in international journals and conferences.