This is an author produced version of a paper published in Northern Lights. This paper has been peer-reviewed but does not include the final publisher proof-corrections or journal pagination.

Citation for the published paper:

Leckner, Sara. (2018). Sceptics and supporters of corporate use of behavioural data : Attitudes towards informational privacy and Internet surveillance in Sweden. Northern Lights, vol. 1, issue 16, p. null

URL: https://doi.org/10.1386/nl.16.1.113_1

Publisher: Intellect

This document has been downloaded from MUEP (<https://muep.mah.se>) / DIVA (<https://mau.diva-portal.org>).

This document is the accepted version, but not the final copyright version of the article:

Leckner, S. (2018), 'Sceptics and supporters of corporate use of behavioural data: Attitudes towards informational privacy and Internet surveillance in Sweden (2018). *Northern Lights* 16 (1): 113-132. doi: 10.1386/nl.16.113_1. For the final published version, please visit: <https://www.intellectbooks.co.uk/journals/view-issue,id=3547/>

Sara Leckner, Dept. of Computer Science and Media Technology, Inst. of Technology and Society, Malmö University, Sweden.

Sceptics and supporters of corporate use of behavioural data: Attitudes towards informational privacy and Internet surveillance in Sweden

abstract

With the growing use of the Internet, companies are increasingly collecting and using personal data for commodifying purposes, resulting in both benefits and privacy risks for users and raising the issue of corporate surveillance. The present article investigates people's attitudes towards corporate collection of personal data, discusses possible reasons for attitude results in relation to self-regulation, trust and media context, and compares these findings with results from the previous year. The study is based on a survey using a large-n probability sample of the Swedish population. The results are in accordance with the suggested privacy paradox: the majority of the population, as in the previous year, have negative attitudes towards corporate collection of their data, largely independent of context. Nonetheless, they continue to share their data without making any great effort to secure their privacy. Whether this depends on inexperience, ignorance or resignation, everyday corporate surveillance does not meet expectations regarding the just governing of informational privacy. As the results showed that the more positive people were towards sharing their data in various contexts, the more positively this affected their attitudes towards the fact that the data were being used by the collecting companies for various purposes, balancing out the power differences online would benefit not only users but also companies to a great extent.

Keywords: personal data privacy data collection monitoring surveillance privacy paradox big data

'Surveillance is the business model of the Internet'

In the present era, when Internet users' personal data have become a valuable commodifying asset, it has been suggested that the primary business model of the Internet is based on mass surveillance, with different Internet actors collecting, storing and using their users' personal data through automated or interactive surveillance processes. And given the basic monetary principles behind this mass surveillance, it can be viewed as a form of economic surveillance:

Facebook uses mass surveillance because it stores, compares, assesses and sells the personal data and usage behaviour of several hundred million users. But this mass surveillance is personalized and individualized at the same time, because the detailed analysis of the interests and browsing behaviour of each user and the comparison to the online behaviour and interests of other users allow Facebook to sort the users into consumer interest groups and to provide each individual user with advertisements that, based on algorithmic selection and comparison mechanisms, are believed to reflect the users' consumption interests. (Fuchs 2017: 195)

Here, surveillance – which in general terms can be described as ‘the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction’ (Lyon 2007: 14) – may be experienced as very similar to, or even synonymous with, data collection and processing as such. The suggested difference is that the concept of surveillance – particularly when it includes the state or organizations – involves power differences, and taking a cue from Foucault’s earlier writings, the concept emphasizes disciplinary power as a form of control rather than a more positive direction or neutral act (Fuchs 2017; Marx 2015). Fuchs (2017) claims that surveillance always involves the systematic use and collection of information in order to dominate individuals or groups, operating overtly as a threat or covertly as an unknown. Marx (2015), however, points out that the modern role of surveillance as control must be viewed in perspective alongside its fundamental importance in enhancing institutional efficiency and services, whereby surveillance is reciprocal and does not only, or necessarily, flow downward or serve to disadvantage. Thus, surveillance is neither good nor bad, but context and comportment can make it either (Marx 2015).

Owing to the widespread, systematic and routine ways in which personal data are possessed and processed today, one can argue that surveillance has become ubiquitous and taken for granted as a simple feature of today’s social life (Lyon 2007) and, according to Giddens (1985), as one of the processes that constitute modernity as such. From a user perspective, generated data from voluntary provision of information online (so-called self-surveillance) can be viewed ‘as a kind of property that a person can own and negotiate’ (Tavani 2008: 134) and just as well become a commodity that can be exchanged for perceived benefits (e.g., Smith et al. 2011). At the same time, ‘being watched over’ often has a negative connotation, and the intensification of corporate data gathering has raised a number of critical issues regarding privacy concerns and inappropriate surveillance, reported by contemporary sources such as mass media (e.g. Teutsch and Niemann 2016; von Pape et al. 2017). The main suggested reason for privacy concerns is lack of control on the part of the user – corporate collection of data is perceived as fair only when the user is granted control over the information and is informed of its intended use – otherwise exercised through such means as approval, modification and the opportunity to opt in or out (Malhotra et al. 2004; Smith et al. 2011). Thus, when asked to provide personal information to corporations, the privacy calculus suggests that consumers often perform a risk–benefit analysis to assess the outcomes they receive in return for their information and respond accordingly (e.g., Smith et al. 2011). But whether these assessments are considered a moderately equal power relationship, or a privacy-impairing ‘necessary evil’ one must agree with in order to participate in the digital society, is another question. There is a fine line between what can be regarded as risk and what can be regarded as beneficial. For example, Facebook’s alleged surveillance, as quoted above, can be perceived both as a threat to the user’s privacy as well as a value-adding service (or a mix thereof).

In order to get a better understanding of how users perceive ubiquitous everyday surveillance on the Internet, the objective of the present article is to examine people’s attitudes towards corporate collection of personal data and how self-regulation, trust and content context affect these attitudes, here focusing on a media industry setting. The article is based on a survey of a large-*n* probability sample of the Swedish population. The purpose is to contribute to the discussion on the relationship between corporate economic surveillance and the public expectation of privacy in relation to the risk–benefit calculus, an area of study that has proved to be both complex and contradictory (see e.g., Baek et al. 2014; Bergström 2015).

Theoretical background

Personal privacy

Privacy can be construed as a need, a right, a condition or an aspect of human dignity (van den Hoven 2008). It has been conceptualized using notions such as ‘freedom from intrusion’, ‘protection of the private sphere’, ‘the right to be left alone’ (Mai 2016a; Solove 2008). Originally, privacy was equated with control per se (e.g. Westin 1967; Altman 1975); however, most evolving definitions equate it with the ability to exert control (Smith et al. 2011). The control-based definition has been mainstream in privacy research, likely because it readily lends itself to the attributes of *informational privacy* (Smith et al. 2011), and very relevant in the context of Internet communication. It is one of several notions of privacy and refers to ‘the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others’ (Westin 1967: 7). The two main conceptualizations of informational privacy, according to Mai (2016a), are ‘privacy as the ability to limit or restrict others from information about oneself’ (e.g., Tavani 2008), and ‘privacy as the control of personal information’ (Solove 2008), both of which assume that privacy is something that can be controlled or restricted in regard to others.

Although personal privacy has gained relevance with the increasing possibilities to collect, process and aggregate user behavioural data, the discussion about informational privacy is not new (see Nissenbaum 1998; Regan et al. 2013; Westin 1967). Registering user behaviour online has long been technically possible, and collection of personal information has been a growing theme in the research literature since the 1970s (Smith et al. 2011). Today, however, measuring technology has become cheaper, and knowledge about big data analysis has increased among Internet actors such as companies and authorities. Additionally, a growing number of people globally are using the Internet, generating an increasing amount of data. As a result, Internet actors have become more interested in the lucrative possibilities offered by collecting and managing personal data, which has fundamentally changed the character of privacy and potential risks of intrusion into it (e.g., Mai 2016a). Yet it is only relatively recently – due to events like Edwards Snowden’s 2013 disclosure of the US intelligence service NSA’s illegal records of people’s use of connected devices worldwide – that corporate data collection and surveillance threats have come to the public’s attention. Despite this and the growing amount of technology available to safeguard or self-regulate personal privacy, there are indications that many people are not fully aware of how and when, and to what extent, Internet actors register personal data (Christensen and Jansson 2015).

Concerns and attitudes towards the collection of personal data

Privacy *concerns* can be connected to privacy *attitudes* (Dienlin and Trepte 2015), described as the ‘evaluative integration of cognitions and affects experienced in relation to an object’ (Crano and Prislin 2006: 347). Privacy *behaviour* is generally described as any observable action by an individual related to optimizing his/her relationship with others, by either limiting self-disclosure or withdrawing from interaction with others (e.g., Dienlin and Trepte 2015; Westin 1967). The connection between attitude and behaviour largely depends on the former (Kaiser et al. cited in Dienlin and Trepte 2015: 287), but different occurrences can change or hinder an individual to actually act in accordance with his or her intention (Eagly and Chaiken 1993). Thus, a person may have a negative attitude, for example towards collection of personal data, but continue to use potentially privacy-impairing services.

Prior studies on people’s positions on corporate collection of personal data have often measured privacy concerns rather than attitudes (e.g., Regan et al. 2013). Privacy concerns measure, for example, whether people are afraid of their Facebook account being compromised – and can only be a negative reaction – whereas privacy attitudes measure whether people believe using Facebook is advantageous or disadvantageous (Dienlin and Trepte 2015). American and European studies have shown that users overall are concerned that they do not have control over their data and that their data may be used in contexts other than those they were originally collected in (EU Commission 2015; Lilley et al. 2012; Pew Research Center 2014), such as third-party use by advertisers and other commercial actors (e.g., Findahl 2014; Kshetri 2014; Narayanaswamy and McGrath 2014; Pew Research Center 2014). But besides being considered as a concern and perceived threat (see also e.g. Bergström 2015; Jansson 2010; Marwick et al. 2017; Pew Research Center 2014), such collection has also been found to be experienced as involving trade-offs for possible benefits, where the price the user pays is increased exposure and registration (Best 2010). And moreover, it has been considered the ‘end of privacy’ (Lyon 2007: 176), where the user simply resigns to it, as registration is thought to be so comprehensive and inevitable that there is no point in trying to understand or fight it (Best 2010; Hargittai and Marwick 2016), and no possibility to opt-out if one wishes to be a part of the digital society. Thus, despite reported concerns about privacy intrusion or experience of lack of control, users continue to use the Internet and behave in ways that seemingly contradict their worries – a phenomenon termed the privacy paradox (e.g., Acquisti cited in Smith et al. 2011: 1000; Bechmann 2014; Dienlin and Trepte 2015). Given the complexity of the subject and that the research on corporate data gathering has generated different results and has often measured privacy concerns, there is a need to further analyse this issue by instead looking at attitudes, which are broader in scope and can be specified for every online privacy action (see also Dienlin and Trepte 2015). Therefore, the present study asks:

RQ1. What are people’s attitudes – in terms of benefits and disadvantages – towards the monitoring and use of their personal data by companies online?

Trust in the process of collection personal data

One prerequisite for commercial Internet actors’ ability to benefit from a data-driven society is public confidence in these actors. Sweden has been described as a ‘high-trust country’, where citizens traditionally have high trust in each other and the institutions of society (Trägårdh et al. 2013; Carlsson and Weibull 2017). The Eurobarometer 2016 (EU Commission 2016) showed that 43 per cent of the Swedish population were not worried about monitoring of their personal data online (see also Dunahee and Lebo 2016). Among the 28 countries in the

European Union, Sweden distinguished itself as the one whose population was the least concerned about the impact of data collection. The situation was basically the same in 2015 (EU Commission 2015). Other comparative international studies have shown that concern about various Internet actors' monitoring of personal data was significantly greater in countries such as the United States, Australia and China than in Sweden (Findahl 2014). Additionally, increased knowledge about privacy and security settings, as well as information about data collection purposes and the ability to modify collected data has been shown to reduce privacy concerns (Jai and King 2016; Leon et al. 2013; Malhotra et al. 2004; Youn 2009). The Swedish population can be considered to have high IT competence, as Sweden was ranked among the top three IT-competent countries in the World Economic Forum's international comparison (World Economic Forum 2015). But, despite the fact that people in Sweden have a high level of trust in different social institutions, are the most positive towards data collection among the European population and have high IT competence compared to people in other countries, *the majority* were concerned about abuse of personal privacy by, for example, corporations (EU Commission 2016) – a finding also confirmed in other studies (e.g., Bergström 2015; Ghersetti 2015).

The perceived trustworthiness of digital services has been found to positively influence people's willingness to share personal data (Chellappa and Sin 2005). Regarding trust in media companies specifically, statistics show that it has been relatively steady among the Swedish population during the past decade, but slightly decreased (Holmberg and Weibull 2016). In 2016, the percentage of the Swedish population stating that they have great or relatively great trust in media companies ranged from 30% (newspapers) to 52% (radio and TV); however, public service TV and radio received higher figures (66% and 70%, respectively). As a comparison, the corresponding figures for authorities such as the police, universities and the government were 53%, 55% and 30% respectively. In 2017, 12% of the population reported great or relatively great trust in Facebook, and 40% reported the same level of trust in Google (Medieakademin 2017). Studies that have looked particularly at trust in relation to the monitoring of personal information by authorities and large media companies (Facebook and Google) confirm that concerns about privacy intrusion have increased slightly during recent years (Findahl 2014). Moreover, trust in sharing one's personal data with companies is related to factors such as friends and acquaintances using the site or service (Bechmann 2014); trust in a company is based on past purchases, subscription and reputation (e.g., Chellappa and Sin 2005; Jai and King 2016; Leon et al. 2013) or on the company's transparency regarding how the collected data will be used (Jai and King 2016; Leon et al. 2013; SAS 2015). Because trust can be a mediating variable between privacy concerns and willingness to disclose information (see e.g., Smith et al. 2011), the following question was posed:

RQ2. To what extent does people's trust in media companies differ from other actors such as authorities?

Users' paradoxical behaviour in relation to privacy concerns according to previous studies

Although users internationally have expressed concerns about lack of control over their data, research suggests that many individuals have not made any major changes in their digital behaviour through self-regulation (Christensen and Jansson 2015; Light and McGrath 2010; Martin et al. 2015). The majority of users in the countries investigated in the World Internet Project believed they had nothing to hide, although an equally high proportion reported that they did protect their data (Lebo 2015). For example, 80% of the Australian population and 70% of the US population stated that they actively protected their personal information; nevertheless, approximately 40% in both countries believed there was no Internet privacy and accepted it (Dunahee and Lebo 2016). In contrast, a majority (81%) of the Swedish population claimed they had not performed any serious self-regulation (e.g., installed virus protection or firewalls or used encryption) to protect themselves from privacy intrusions and involuntary surveillance, although 52% stated that they could control their privacy and 53% that they did so to some extent (e.g., cleared their cache memory or used ad-blockers) (Findahl 2014). Reasons for lack of self-regulation include inadequate knowledge of how and when data are gathered as well as of how to protect oneself and belief that one has nothing to hide (e.g., Findahl 2014; Light and McGrath 2010; Martin et al. 2015). Moreover, studies have shown that users often submit digital consent without reading the terms and conditions (e.g., Alverén 2012; Bechmann 2014; Mai 2016a; Pitkänen and Tuunainen 2012). For example, only one-fifth of Europeans fully read privacy statements, according to the Eurobarometer 2015 (EU Commission 2015). As consumer privacy is strongly related to the ability to control one's privacy, and as research has found 'the stronger an individual's concerns are about corporate collection practices, the more likely the individual is to adopt risk-reducing behaviours' (Youn 2009: 392), the following question was posed:

RQ3. To what extent have people performed self-regulation regarding the monitoring of their data?

Privacy in relation to context and control

Many theories assume that privacy is something that can be controlled, as previously mentioned. Several scholars, however, argue that full control cannot be achieved online and that all surveillance systems are not viewed with the same mistrust, instead privacy should be regarded as contextual (e.g., Acquisti cited in Smith et al. 2011: 1002; Nissenbaum 2015). Nissenbaum's (2015) theory of *contextual integrity* holds that the source of user anxiety over privacy is neither control nor secrecy, but rather appropriateness. Contexts like technologies and applications, type of information, sectors and practices that disrupt privacy are the ones that result in inappropriate flows of personal information, violating context-specific informational norms: information types, actors and transmission principles. Whether a particular flow is appropriate depends on the norms and conditions or constraints under which the transmission takes place (Nissenbaum 2015). For example, sharing information with a friend on Facebook must be judged in relation to different norms than sharing the same information with a commercial company (see Fuchs 2017). Nissenbaum also points out that control over information is one among an extensive range of possible transmission principles, for example 'with third-party authorization', 'as required by law', 'bought', 'sold', etc., arguing that contextual integrity offers the best way to protect privacy.

Prior research has found that consumer beliefs and behavioural responses to privacy – concerns or willingness to share – depend on aspects such as sector, as mentioned, but also on type of information. Data on media use, e-commerce or other lifestyle characteristics have been found to be considered less sensitive to share (e.g. EU Commission 2011; SAS 2015), compared to information like social security numbers, credit card numbers, and health and medical data (Jai and King 2016; Leon et al. 2013; PriceWaterCoopers 2012; SAS 2015). These findings are supported by earlier studies (see e.g., Malhotra et al. 2004). Concerning media-related information specifically, Leckner and Appelgren (2015) investigated the type of information users were willing to disclose. The results indicated that users were more willing to share information from media activities involving less interaction and intimacy, such as visited news sites or streamed movie content, than information from activities involving a higher degree of interactivity, such as social media use. The majority of the participants in the study did not want to share information about personal communication, such as e-mail. Altogether, very few wanted to share information from all their Internet activities. Given that the industry to which an organization belongs as well as type of information can be viewed as contextual variables (see also Malhotra et al. 2004; Smith et al. 2011) and that these variables may influence user attitudes, the following question was posed:

RQ4. To what extent are people's attitudes towards the monitoring and use of their personal data dependent on the media company and its contextual offerings?

Why people engage in paradoxical behaviour and behaviour changes over time

Various theories have suggested that there are several reasons why a person might engage in paradoxical behaviour. One reason is a gap between behaviour and attitude. A number of boundary conditions concerning why and when this gap occurs have been proposed (see e.g. Dienlin and Trepte 2015). The first condition states that the connection between attitude and behaviour largely depends on the former, where knowledge has been found to have a great influence on attitudes towards behaviour (Fabrigar et al. 2006). The second condition addresses personal experiences, which determine whether attitudes will enable adequate predication of behaviour. For example, many people may not have experienced privacy violation themselves; for such people, privacy attitudes may be based largely on intuition or second-hand experience (e.g., Dienlin and Trepte 2015; Malhotra et al. 2014). Although lack of first-hand experience may result in authentic concerns, it may not be consolidated enough to influence subsequent behaviour, as personal experience is important for building sustainable attitudes (see e.g. Tormala et al. cited in Dienlin and Trepte 2015: 287). Moreover, attitudes based on a high level of knowledge are more likely to be stable between the time of assessment of the attitude and the behaviour (Fabrigar et al. 2006). A further condition pointed out is that when a person is asked to express his/her attitude, the attitude may have been influenced (e.g., by subjective norms, peer pressure, self-denial), causing the person to withhold information or provide false information (Dienlin and Trepte 2015). One important contemporary influence is mass media, which have often been found to focus on prevailing privacy risks (Teutsch and Niemann 2016; von Pape et al. 2017). Consequently, the respondents' answers may largely reflect public opinion rather than their own personal opinion. Thus, there is reason to believe that Internet users' attitudes towards personal data are affected over time, particularly because people tend to adopt new technologies more easily when they become common or normal within our social network systems (Christensen 2016; Jansson 2010). Based on this, the following question was asked:

RQ5. To what extent have people's attitudes towards monitoring and use of their personal data changed since the previous year (2015)?

Method

This study is based on survey data collected during the autumn and winter of 2015 and 2016 through the Swedish national Society, Opinion, Media (SOM) survey, conducted annually since 1986. The survey (distributed via mail and online) was used to gather a systematic representative sample of the Swedish population aged 16–85. The part of the survey relevant to this study was sent to 3400 individuals in 2015 and 2016, with a net response rate of 51 per cent in 2015 and 53 per cent in 2016. The sample consisted of both users and non- users of the Internet (i.e., those who stated they had and had not used the Internet during the past twelve months).

The questions used in the surveys focused on attitudes towards privacy on the Internet. The respondents were asked to rate: (1) the extent to which they limit the information about themselves that they post online; (2) whether they carefully read terms and conditions when they register for services on websites or mobile phone apps; (3) whether it is good that companies collect information about their Internet behaviour to improve services and (4) whether they accept that the information that companies collect about them on the Internet is sold to third parties. In the 2016 survey, another question was added: whether they make active choices in order to surf anonymously. The respondents rated their attitudes on a four- point scale, ranging from 'Completely agree' to 'Completely disagree'. The option 'No opinion' was also available. The respondents were also asked about their attitudes towards collection of personal data depending on the media actor and the context to which the actor's service related. These five contexts were: search engines, online news, social media and streaming movies and TV series. In the 2016 survey, another item was added to allow comparison with a non-commercial actor: government. A five-point scale was used with options ranging from 'Very negative' to 'Very positive'. The option 'No opinion' was also available. The questions were analysed using frequency analysis, Pearson Correlation Coefficient and Independent Samples *t*-test.

Furthermore, the respondents were asked about their level of trust of 'authorities' and 'media companies'. 'Authorities' consisted of five items: government, police, defense, courts and universities, and 'Media companies' consisted of: press; and radio and TV. The respondents rated their attitudes on a five-point scale, ranging from 'Completely agree' to 'Completely disagree'. The question was analysed through a Sum score non-parametric test, using Wilcoxon Signed-Rank.

Results

RQ1 asked what attitudes people had regarding corporate collection of their personal data. Few believed it was beneficial to share data with commercial actors on the Internet: 18% fully or partially agreed with this claim, compared to 60% who did not (Table 1). In addition, the majority (58%) were negative towards their data being sold to third parties, compared to 26% who fully or partially accepted it. Moreover, although collected personal data can have many benefits for individuals, the majority (58%) did not agree with the statement that it was good that actors collected data in order to improve websites and services (Table 1).

Table 1: Attitudes towards the collection of personal data online (%).

	Totally agree	Partly agree	Partly disagree	Totally disagree	No opinion	N
Good that companies collect data to improve services	3	21	20	38	18	1,623
Accept that data are sold to third parties	5	21	17	41	16	1,628
Benefits of collecting data outweigh disadvantages	3	15	21	39	22	1,620

Table 2: Measures to protect personal privacy online (%).

	Totally agree	Partly agree	Partly disagree	Totally disagree	No opinion	N
Make active choices to surf anonymously	8	23	16	25	28	1,614
Carefully read agreements when registering on sites and apps	14	30	20	20	16	1,629

RQ2 asked about people's trust in media companies compared to authorities. The results showed that people had significantly higher trust in authorities than in media companies in both 2015 ($z=32.718$, $N\text{-ties}=1419$, $p=0.000$) and 2016 ($z=33.093$, $N\text{-ties}=1456$, $p=0.000$).

RQ3 asked about the extent to which people had performed self-regulation to protect their privacy. Approximately one-third claimed they made active choices in order to surf anonymously, compared to 41 per cent who did not (Table 2). Nearly 30 per cent stated that they had no opinion, and it is likely that these people also did not actively protect their privacy. However, what 'active choice' meant could not be determined from the present study.

Table 3: Correlation between questions regarding the digital registration of personal information (Pearson's r).

	Carefully read agreements	Accept that data are sold to third parties	Good that companies collect data to improve services	Benefits of collecting data outweigh disadvantages	Make active choice to surf anonymously
Carefully read agreements	1				
Accept that personal data are sold to third parties	-0.054	1			
Good that companies collect data to improve services	0.016	0.394**	1		
Advantages of companies' collection outweigh disadvantages	0.002	0.441**	0.756**	1	
Make active choices to surf anonymously	0.192**	-0.050	-0.062*	-0.038	1

Note: * $p<0.05$, ** $p<0.01$. Significant correlations above 0.2 are shown in bold. N who answered 'No opinion' have been excluded.

Similar to taking measures to surf anonymously, having a negative attitude towards corporate collection of personal data did not affect how well people read terms and conditions describing what companies do with the collected data. About as many (44 per cent) stated they carefully read policy agreements as those (40 per cent) who stated they did not (Table 2).

A correlation analysis showed a strong positive relation between the attitude that 'it was good that companies collected data in order to improve services' and 'believing that the benefits of companies collecting data outweigh the disadvantages' (Table 3). Moreover, a relatively strong positive correlation was found between 'accepting that data were sold to third parties' and 'considering that the benefits of corporate collection of data outweigh the disadvantages', as well as 'being positive to collection being done to improve services'. This indicates that people who are positive towards data collection in general, also are positive towards that data were it being used for different purposes by the collecting actors, regardless if it was to improve services or resell the collected data. And the opposite: the more positive were also positive about that data were being used for different purposes. The questions with no or weak correlations concerned protecting one's privacy. The significant correlations

indicated that people who were negative towards the collection of data, also agreed to be more restrictive and more careful with their data online.

RQ4 asked about the extent to which people's attitudes towards monitoring were dependent on context, in this case type of media sector and its offered content. The results showed that attitudes were context dependent. People were the least negative towards collection during the use of streaming TV and movie services (e.g., Netflix, HBO), compared to search engine companies (e.g., Google, Firefox), news companies (e.g., public service, news- paper companies) and social media companies (e.g. Facebook, Twitter) (see Table 4). Comparing the media industry's collection with that of authorities', people were foremost neutral (neither positive nor negative) towards collection by authorities (33 per cent), whereas they were clearly negative towards collection by media companies (Table 4). Altogether, the number of respondents who were negative towards corporate monitoring of personal data was larger than those who were positive, but about equal to the number of people who were neither negative nor positive and did not take a stand. The latter figure was particularly large for the streaming TV and movie context, where 56 per cent stated 'no opinion' or 'neither positive nor negative'. The reason for this finding is not obvious, but can be related to people's feeling that that type of information is considered less 'sensitive' to share, or that these types of services are less diffused among the population, compared to the other contexts.

Independent of the examined media context, a correlation analysis showed relatively strong, significant, positive correlations between the 'benefits of collection outweighing the disadvantages', as well as for attitudes towards the 'registration of data aimed at improving the actors' services' (Table 5). Significant but slightly weaker positive relationships were also apparent for 'accepting data being sold', with the weakest correlation to authorities' collection of personal data. This indicates that people who were positive towards registration of personal data in general, were positive towards this being done in the media business contexts included in the present study. And the opposite: people who are negative towards registration in general are negative towards registration in the investigated contexts. Moreover, similar to Table 3, the items with weaker negative and non-significant correlations were related to protecting one's privacy. The significant, and negative, correlations indicated that people who are less inclined to read agreements and make active choices, are those with a more positive attitude towards the actors' collection. And the opposite: people with a negative attitude are more inclined to take precautions. For example, those who are negative towards search engine and social media companies' registrations are more likely make active choices to surf anonymously, whereas those who are positive towards registration during film and TV streaming are less likely to read agreements carefully.

Table 4: Attitudes towards different Internet actors registering personal data when one uses their Internet sites and services (%).

Type of actor	Very positive	Rather positive	Neither positive nor negative	Rather negative	Very negative	No opinion	Balance measure	N
Authorities	6	19	33	11	16	15	-2	1,625
News	2	5	26	20	25	22	-38	1,629
Search engines	3	11	29	21	23	13	-30	1,623
Social media	2	6	23	20	26	23	-38	1,622
Film/TV streaming	4	11	21	11	18	35	-14	1,622

Note: The balance measure between -100 and +100 is the number of people who answered *Very/Rather positive* minus the number who answered *Very/Rather negative*. -100 means that all consider it negative and +100 that all consider it positive.

RQ5 asked about the extent to which the users' attitudes towards the monitoring and use of their personal data had changed between 2015 and 2016. Comparing the results from the two years, people were still mainly negative towards corporate collection of personal data in 2016, as they had been in 2015; however, a slight change in attitudes between the years can be noted. The extreme values decreased in 2016: both the very positive and the very negative values in 2015 seemed to have moved towards a somewhat more neutral attitude. In 2016, people had become slightly less negative towards data being collected to improve the sites and services a company offers ($F=7.51$, $p<0.001$), and accepted to a greater extent collected data being sold to third parties ($F=0.07$, $p<0.01$).

However, in 2016 there were still three times as many who did not believe that the benefits of corporate data collection outweighed the disadvantages, as shown in Table 1. The issue of whether people performed self-regulation in order to surf anonymously was not measured in 2015, and the extent to which people carefully read terms and agreements when registering on sites or apps showed no significant difference between the two years.

Table 5: Correlations between attitudes towards corporate registration of personal data using Internet services and different contexts (Pearson's r).

	News	Authorities	Search engine	Social media	Film/TV streaming
Carefully read agreements	0.036	-0.023	-0.036	0.008	-0.135***
Accept that personal data are sold	0.260***	0.195***	0.279***	0.245***	0.276***
Good that companies collect data to improve services	0.464***	0.320***	0.481***	0.467***	0.421***
Benefits of companies collecting data outweigh disadvantages	0.424***	0.285***	0.452***	0.430***	0.382***
Make active choices to surf anonymously	-0.038	-0.022	-0.092**	-0.081**	-0.034

Note: ** $p < 0.01$, *** $p < 0.001$. Significant correlations above 0.2 are shown in bold. *N* who answered 'No opinion' have been excluded.

Results related to context were not comparable, because the questions regarding this issue diverged somewhat between the two surveys. What can be determined is that, in contrast to 2016, the results from 2015 showed no significant differences in people's attitudes concerning business context. Instead, people were rather consistently negative towards corporate collection regardless of context. In 2016, however, people had become somewhat less negative towards such monitoring, as shown in Table 4. Altogether, the results indicate that people had become slightly less negative towards corporate collection of personal data the last year – not more positive but to a higher extent more neutral, that is, neither positive nor negative.

Discussion

The present article investigates people's attitudes towards corporate collection of data, specifically how attitudes are related to self-regulation, trust and media business contexts. The article also examines whether these attitudes changed from the previous survey year (2015) to the next (2016).

In the study, attitudes were not identical to behaviour. The results showed that the majority of the Swedish population had negative attitudes towards Internet actors monitoring and using their personal data. Benefits, such as sharing data to improve sites and services, were not considered to outweigh the risks, such as personal information being sold to third parties. The negative attitudes indicate a non-correspondence with people's actual Internet behaviour, as 93 per cent of the Swedish population used the Internet the year the study was conducted (Davidsson and Findahl 2016). Moreover, despite a negative attitude, almost two-thirds made no active choice to surf anonymously. And although close to half the population in the present study agreed that they carefully read terms and conditions when registering on sites and apps, almost the same number of people did not, and there was no significant difference from the previous year. These results are similar to other studies showing that associations between privacy concerns and stated intentions may not be reflected in actual behaviour, the reason for the emergence of the term the privacy paradox.

What might be reasonable explanations for this paradoxical behaviour? One is a lack of knowledge on the part of many users concerning when, where, by whom and for what purposes personal data are actually collected online. Lyon (2014) argues that one reason is that Internet surveillance today is hidden in its presence; in part, this has to do with the increasingly technological character of surveillance, whereby technology itself is gradually disappearing from sight and becoming more ubiquitous, at the same time as it becomes more powerful. Thus, the

collection process is ambiguous to the user (see also Borgesius 2015). Although users are informed through policies and agreements of what they are agreeing to let companies do with their personal data when they give digital consent, according to the present findings it is likely that in practice the majority do not read them, and it is questionable how many actually understand what they are agreeing to. The ubiquitousness of corporate surveillance and the increasing everyday use of the Internet also make the privacy calculus – assessing the outcomes received in return for personal data – a rather routine performance, whereby the benefits of opting in are higher than not being able to take part in the digital society, but whereby privacy is negotiated away or even repressed. This does not mean that corporate collection of personal data is perceived as fair and that users believe they have control, however, as indicated by the negative attitudes shown in the present study.

Independent of whether the acceptance of corporate collection depends on inexperience and unawareness of the collection process, on ignorance or neglect of possible consequences or on resignation to the impossibility of opting out, it means that people cannot make rational decisions regarding what information is appropriate to share and may make decisions that go against their expected norms, resulting in privacy concerns (cf. Nissenbaum 2015). As privacy theories suggest that people's willingness to share personal data is related to the extent to which they have control over these data, companies need to develop their systems so that consumers have the power to adapt their sharing to their individual preferences in a transparent manner (see also Evens and Van Damme 2016). Although total control over personal data may not be possible in practice, companies need to emphasize the benefits of sharing to consumers, so that corporate collection becomes a less negative issue.

But to some extent, attitudes depend on context. Although Sweden, from an international perspective, is a country whose citizens have high trust in the institutions of society, people nevertheless had overall negative attitudes towards corporate collection independent of context; nevertheless, some differences were found. Whereas attitudes towards the media sector's collection of personal data were found to be clearly negative, people were slightly more neutral regarding monitoring by authorities. This was confirmed by findings showing an overall higher trust in the latter sector. Thus, it can be expected that this sector met the expectations regarding governing the flow of personal information to a higher extent, and produced less of 'a schism between experience and expectation' (Nissenbaum 2010: 231). However, it can be argued that individuals will not necessarily perceive their privacy as being violated if control and access are not particularly important features of that context; thus, attitudes can depend on the type of information within a sector. In the present study, differences in attitudes depending on the media sector were found, similar to prior reports on the perceived trust of different sectors (see Holmberg and Weibull 2016; Medieakademin 2017). The streaming TV and film context generated the least negative attitudes. These are neither directly personal nor 'sensitive' data, in the sense that it involves content concerning leisure rather than work and public affairs, compared to the other measured contexts – search engines, news sources and social media – which, in that order, were associated with increasingly negative attitudes. Moreover, the results indicated that if an individual was more positive towards sharing data in various contexts, this also positively affected his/her attitude towards data being sold and collected to improve the user experience. This lends support to the notion that companies would benefit from introducing measures that to a higher extent encourage consumers to adopt more positive attitudes towards sharing data.

Nonetheless, the results showed that the Swedish population has become slightly less negative towards data collection compared to 2015. This does not mean they have become more positive but rather less negative, adapting a more neutral state of being neither positive nor negative. It can indicate that Internet users' attitudes towards the collection of personal data are changing, although the results should be interpreted with caution as the measurement currently covers only two years. However, in any society, there is always a certain proportion of people who are skeptical of the new and unknown (Rogers 2003), not least new technologies. When a technology becomes more assimilated in society the experience of violated norms of distribution decreases, causing people to adjust their behaviour to their own benefit (Lipford et al. 2009). Increased knowledge about privacy and security settings, as well as information about data collection purposes and the ability to modify collected data, has been shown to reduce privacy concerns. But, despite the fact that, from an international perspective, people in Sweden have a high trust in social institutions, have high IT competence, and are the most positive towards data collection among the European population, the majority is still negative towards corporate data collection; this may indicate that Internet technology is nonetheless not yet fully diffused in Sweden. Some of the challenges of everyday corporate surveillance can be due to this and will thus likely decrease when a larger share of the population have become more accustomed to Internet technology, including increased knowledge of the data collection process and self-regulation settings.

Limitations

The above-mentioned inexperience and potential lack of knowledge about everyday surveillance are also related to the limitations of the present study, particularly the methodology used. When people are asked to express their attitudes these can be influenced, implicitly or explicitly, causing them to provide untrue or modified information (Dienlin and Trepte 2015). When people answer a survey, they seldom retrieve all relevant information from memory or think through their opinions in depth. Instead, their answers tend to be based on the most available information; that is, that which was stored or activated most recently (Strömbäck 2009). If people lack knowledge of the process of Internet surveillance and data collection in practice, as suggested in the present study, their attitudes are not consolidated enough to influence subsequent behaviour, as suggested by attitude-behaviour theories. Possible reasons for this include that the respondents' opinions may not be based on their own personal experiences but rather on intuition or second-hand experience, for example from contemporary mass media reports. Consequently, user attitudes might largely reflect public opinion rather than personal opinion. Thus, there was no knowledge of the extent to which the respondents knew the scope of data collection taking place prior to the study, although different contexts and brief examples were given in conjunction with the survey questions. In line with this, phrasing questions about privacy is complicated, as previously discussed with regard to attitude versus privacy concerns. For example, how a respondent is asked about his/her attitude – 'do you want to be tracked?' or 'do you agree to share your data?' – will likely generate different answers; hence, it is difficult to experimentally measure knowledge (e.g., Fabrigar et al. 2006; Regan et al. 2013). However, the questions in the surveys were formulated with this challenge in mind. Nevertheless, it is possible that the respondents' concerns may have been exaggerated when they responded and that this was reflected in the large proportion of people with negative attitudes towards the collection of personal data. Moreover, the topic under study is multifaceted and complex, and the respondents may have used different constructs and thus considered different aspects regarding privacy and data collection when answering the surveys (cf. Regan et al. 2013).

Conclusion

In a way, the relationship between corporations and consumers regarding the issue of Internet surveillance can be seen as a matter of the chicken or the egg. The better and more accurate search results, personalized ads and content are, the more likely it is that users will use a company's services. And the more they use these services, the more data about them can be (and are) collected, stored and assessed. Marx (2015) argues that, in our media-saturated, communication-intensive and visual world, many people want to see and be seen, at the same time as they want to be able to look away and be left alone; we want to know, but also to be shielded from knowing. One can argue that users' permanent, and currently rather uncritical, use of the Internet and input of personal data support the situation of corporate monitoring and commodification, and serve as a prerequisite for Internet surveillance to work (see Fuchs 2017). On the other hand, control over one's privacy is not something the individual should have to assume full responsibility for; it goes beyond the individual level, to society (see Mai 2016b; Solove 2008). Although current forms of surveillance increasingly depend on the compliant exchange of user information and corporate services, as suggested by Christensen (2016), corporations still have the upper hand in this relationship. From the users' perspective, corporate data collection is currently regarded as something negative, largely independent of context. On the increasingly important economic Internet market, companies have a great responsibility to even out the power differences in the process of collecting personal data, in order to support a more equal exchange of information.

Acknowledgement

Thanks to Ester Appelgren and the SOM Institute for support and participation during the implementation of this study.

References

- Altman, I. (1975), *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*, Monterey: Brooks and Cole Publishing Company.
- Alverén, F. (2012), *Såld på nätet: priset du betalar för gratis* ('Sold online: The price you pay for free'), Stockholm: Ordfront.
- Baek, Y.M., Kim, E.M. and Bae, Y. (2014), 'My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns', *Computers in Human Behavior*, 31, pp. 48–56.

Bechmann, A. (2014), 'Non-informed consent cultures: Privacy policies and app contracts on Facebook', *Journal of Media Business Studies*, 11:1, pp. 21–38.

Bergström, A. (2015), 'Online privacy concerns: Abroad approach to understanding the concerns of different groups for different uses', *Computers in Human Behavior*, 53, pp. 419–26.

Best, K. (2010), 'Living in the control society: Surveillance, users and digital screen technologies', *International Journal of Cultural Studies*, 13:1, pp. 5–24.

Borgesius, F. J. Z. (2015), 'Personal data processing for behavioural targeting: Which legal basis?', *International Data Privacy Law*, 5:3, pp. 163–76.

Carlsson, U. and Weibull, L. (2017), *Yttrandefriheten i dagens mediekultur: En studie av medborgarnas uppfattning om yttrandefrihetens gränser* ('Freedom of expression in today's media culture'), Göteborg: Nordicom, Göteborgs Universitet.

Chellappa, R.K. and Sin, R.G. (2005), 'Personalization versus privacy: An empirical examination of the online consumer's dilemma', *Information Technology Management*, 6:2&3, pp. 181–202.

Christensen, M. (2014), 'Technology, place and mediatized cosmopolitanism', in A. Hepp and F. Krotz (eds), *Mediatized Worlds: Culture and Society in a Media Age*, New York: Palgrave MacMillan, pp. 159–73.

—— (2016), 'Cultures of surveillance: Privacy and compliant exchange', *Nordicom Review*, 37, pp. 177–82.

Christensen, M. and Jansson, A. (2015), *Cosmopolitanism and the Media: Cartographies of Change*, New York: Palgrave MacMillan.

Crano, W. D. and Prislin, R. (2006), 'Attitudes and persuasion', *Annual Review of Psychology*, 57:1, pp. 345–74.

Davidsson, P. and Findahl, O. (2016), *Svenskarna och internet 2016* ('The Swedes and the Internet 2016'), Internetstiftelsen i Sverige, https://www.iis.se/docs/Svenskarna_och_internet_2016.pdf. Accessed 18 August 2017.

Dienlin, T. and Trepte, S. (2015), 'Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors', *European Journal of Social Psychology*, 45:3, pp. 285–97.

Dunahee, M. and Lebo, H. (2016), *World Internet Project International Report*, 6th ed., Los Angeles: Center for the Digital Future, University of Southern California.

Eagly, A.H. and Chaiken, S. (1993), *The Psychology of Attitudes*, Fort Worth, TX: Harcourt Brace & Company.

EU Commission (2011), 'Attitudes on data protection and electronic identity in the European Union (Special Eurobarometer 359)', http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf. Accessed 7 May 2016.

—— (2015), 'Data protection (Special Eurobarometer 431)', <http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/yearFrom/2015/yearTo/2017/surveyKy/2075>. Accessed 28 April 2017.

—— (2016), 'Online platforms (Special Eurobarometer 447)', <http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/yearFrom/2015/yearTo/2017/surveyKy/2126>. Accessed 28 April 2017.

Evens, T. and Van Damme, K. (2016), 'Consumers' willingness to share personal data: Implications for newspapers' business models', *International Journal of Media Management*, 18:1, pp. 24–41.

Fabrigar, L.R., Petty, R.E., Smith, S.M. and Crites Jr, S.L (2006), 'Understanding knowledge effects on attitude-behavior consistency: The role of relevance, complexity, and amount of knowledge', *Journal of Personality and Social Psychology*, 90:4, pp. 556–77.

Findahl, O. (2014), 'Svenskarna och internet 2014' ('The Swedes and the Internet 2014'), <http://www.soi2014.se>. Accessed 18 August 2017.

Fuchs, C. (2017), *Social Media: A Critical Introduction*, 2nd ed., London: Sage.

Ghersetti, M. (2015), 'Sociala medier till njä och nytta' ('Social media for pleasure and benefit'), in A. Bergström, B. Johansson, H. Oscarsson and M. Oskarson (eds), *Fragment*, Göteborg: SOM-institutet vid Göteborgs universitet, pp. 511–22.

Giddens, A. (1985), *The Nation-State and Violence*, Berkeley: University of California Press.

Hargittai, E. and Marwick, A. (2016), '“What can I really do?” Explaining the privacy paradox with online apathy', *International Journal of Communication*, 10, pp. 3737–57.

Holmberg, S. and Weibull, L. (2016), 'Långsiktiga förändringar i svenskt institutionsförtroende' ('Long-term changes in Swedish institutional trust'), in A. Andersson, J. Ohlsson, H. Oscarsson and M. Oskarson (eds), *Larmar och gör sig till*, Göteborg: SOM-institutet vid Göteborgs universitet, pp. 39–57.

Hoven, J. van den (2008), 'Information technology, privacy and the protection of personal data', in M. J. van den Joven and J. Weckert (eds), *Information Technology and Moral Philosophy*, Cambridge: Cambridge University Press, pp. 301–21.

Jai, T.M. and King, N.J. (2016), 'Privacy versus reward: Do loyalty program increase consumers' willingness to share personal information with third-party advertisers and data brokers?', *Journal of Retailing and Consumer Services*, 28, pp. 296–303.

Jansson, A. (2010), 'Integritetsrisker och nya medier' ('Privacy risks and new media'), in S. Holmberg and L. Weibull (eds), *Nordiskt ljus: trettiosju kapitel om politik, medier och samhälle*, Göteborg: SOM-institutet, pp. 261–76.

Kshetri, N. (2014), 'Big data's impact on privacy, security and consumer welfare', *Telecommunications Policy*, 38:11, pp. 1134–45.

Lebo, H. (2015), *The 2015 Digital Future Report*, Los Angeles: Annenberg School, Center for the Digital Future, University of Southern California.

Leckner, S. and Appelgren, E. (2015), 'The audience's willingness to share internet traffic data: An emerging ethical challenge for the media industry', *NordMedia 2015*, Copenhagen, 13–15 August.

Leon, P.G., Ur, B., Wang, Y., Sleeper, M., Balebako, R., Shay, R., Bauer, L., Christodorescu, M. and Cranor, L.F. (2013), 'What matters to users? Factors that affect users' willingness to share information with online advertisers', *Symposium on Usable Privacy and Security (SOUPS) 2013*, Newcastle, 24–26 July.

Light, B. and McGrath, K. (2010), 'Ethics and social networking sites: A disclosive analysis of Facebook', *Information, Technology and People*, 23:4, pp. 290–311.

Lilley, S., Grodzinsky, F.S. and Gumbus, A. (2012), 'Revealing the commercialized and compliant Facebook user', *Journal of Information, Communication and Ethics in Society*, 10:2, pp. 82–92.

Lipford, H., Hull, G., Latulipe, C. and Watson, J. (2009), 'Visible flows: Contextual integrity and the design of privacy mechanisms on social network sites', *12th IEEE International Conference on Computational Science and Engineering*, Vancouver, 29–31 August.

Lyon, D. (2007), *Surveillance Studies: An Overview*, Cambridge: Polity Press.

- (2014), 'The emerging surveillance culture', in A. Jansson and M. Christensen (eds), *Media, Surveillance and Identity: Social Perspectives*, New York: Peter Lang Publishing, Inc., pp. 71–90.
- Mai, J.-E. (2016a), 'Three models of privacy. New perspectives on informational privacy', *Nordicom Review*, 37, pp. 171–75.
- (2016b), 'Big Data privacy: The datafication of personal information', *The Information Society*, 32:3, pp. 192–99.
- Malhotra, N., Kim, S. and Agarwal, J. (2004), 'Internet Users' Information Privacy Concerns (IUIPC): The construct, the scale, and a causal model', *Information Systems Research*, 15:4, pp. 336–55.
- Martin, S., Rainie, L. and Madden, M. (2015), 'Americans' privacy strategies post-Snowden', Pew Research Center, <http://www.pewinternet.org/2015/03/16/Americans-Privacy-Strategies-Post-Snowden/>. Accessed 17 April 2017.
- Marwick, A., Fontaine, C. and boyd, d. (2017), '"Nobody sees it, nobody gets mad": Social media, privacy, and personal responsibility among low-SES youth', *Social Media + Society*, 3:2, pp. 1–14.
- Marx, G.T. (2015), 'Surveillance studies', *International Encyclopedia of the Social and Behavioral Sciences*, 2:23, pp. 733–41.
- Medieakademien (2017), 'Medieakademins förtroendebarmeter 2017' ('The Media Academy's trust barometer 2017'), Göteborgs universitet och TNS-Sifo, <http://medieakademien.se/wp-content/uploads/2017/04/Fortroendebarmetern2017.pdf>. Accessed 28 September 2017.
- Narayanaswamy, R. and McGrath, L. (2014), 'A holistic study of privacy in social networking sites', *Journal of Management Information and Decision Sciences*, 17:1, pp. 71–85.
- Nissenbaum, H. (1998), 'Protecting privacy in an information age: The problem of privacy in public', *Law and Philosophy*, 17:5&6, pp. 559–96.
- (2010), *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford: Stanford University Press.
- (2015), 'Respecting context to protect privacy: Why meaning matters', *Science and Engineering Ethics*, pp. 1–22.
- Pape, T. von, Trepte, S. and Mothes, C. (2017), 'Privacy by disaster? Press coverage of privacy and digital technology', *European Journal of Communication*, 32:3, pp. 189–207.
- Pew Research Center (2014), 'Public perceptions of privacy and security in the post-Snowden era', <http://www.pewinternet.org/2014/11/12/public-privacy-perceptions>. Accessed 21 April 2017.
- Pitkänen, O. and Tuunainen, V.K. (2012), 'Disclosing personal data socially: An empirical study on Facebook users' privacy awareness', *Journal of Information Privacy & Security*, 8:1, pp. 3–29.
- PriceWaterCoopers (2012), 'Consumer privacy: What are consumers willing to share', Consumer Intelligence Series, PriceWaterCoopers, <http://www.pwc.com/us/en/industry/entertainment-media/publications/consumer-intelligence-series/consumer-privacy.jhtml>. Accessed 21 April 2016.
- Regan, P.M., FitzGerald, Gerald and Balint, Peter (2013), 'Generational views of information privacy?', *Innovation: The European Journal of Social Science Research*, 26:1&2, pp. 81–99.
- Rogers, E.M. (2003), *Diffusion of Innovations*, 3rd ed., New York: The Free Press. SAS (2015), 'Finding the right balance between personalization and privacy', research paper, Cary, NC: SAS Institute.
- Smith, J.H., Dinev, T. and Xu, H. (2011), 'Information privacy research: An interdisciplinary review', *MIS Quarterly*, 35:4, pp. 989–1015.

Solove, D. (2008), *Understanding Privacy*, Cambridge: Harvard University Press.

Strömbäck, J. (2009), *Makt, medier och samhälle* ('Power, media and society'), Stockholm: SNS Förlag.

Tavani, H.T. (2008), 'Informational privacy: Concepts, theories, and controversies', in K. E. Himma and H. T. Tavani (eds), *The Handbook of Information and Computer Ethics*, Hoboken: John Wiley & Sons, pp. 131–65.

Teutsch, D. and Niemann, J. (2016), 'Social network sites as a threat to users' self-determination and security: A framing analysis of German newspapers', *The Journal of International Communication*, 22:1, pp. 22–41.

Trägårdh, L., Wallman Lundåsen, S., Wollebæk, D. and Svedberg, L. (2013), *Den svala svenska tilliten* ('The cool Swedish trust'), Stockholm: SNS Förlag.

Westin, A.F. (1967), *Privacy and Freedom*, New York: Atheneum.

World Economic Forum (2015), *ICTs for Inclusive Growth, The Global Information Technology Report 2015*, Geneva: World Economic Forum.

Youn, S. (2009), 'Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents', *Journal of Consumer Affairs*, 43:3, pp. 389–418.