Digital Journalism

ISSN: 2167-0811 (Print) 2167-082X (Online) Journal homepage: http://www.tandfonline.com/loi/rdij20

Not Interesting Enough to be Followed by the NSA

Anouk Mols & Susanne Janssen

To cite this article: Anouk Mols & Susanne Janssen (2017) Not Interesting Enough to be Followed by the NSA, Digital Journalism, 5:3, 277-298, DOI: 10.1080/21670811.2016.1234938

To link to this article: http://dx.doi.org/10.1080/21670811.2016.1234938

NOT INTERESTING ENOUGH TO BE FOLLOWED BY THE NSA
An analysis of Dutch privacy attitudes

Anouk Mols and **Susanne Janssen**

Open curtains and a careless attitude. The Dutch are described as holding an indifferent stance towards privacy in the aftermath of Snowden's revelations of far-reaching government surveillance. But are Dutch reactions as aloof as often claimed? This study provides an in-depth overview of privacy attitudes in the Dutch debate about the National Security Agency (NSA) leaks, showing a greater variety of sentiments than anticipated. A qualitative frame analysis and a quantitative descriptive analysis resulted in six frames, which convey distinct privacy attitudes. Online and offline as well as professional and non-journalistic content in the debate displays a different distribution of frames. The frames, ranging from an "End justifies the means" attitude to an anxious fear of an "Orwellian dystopia", are placed in a larger framework as the research demonstrates the connection to existing theories about privacy and surveillance. Dutch discussions about the NSA revelations often display a trade-off narrative balancing safety against privacy, and include (de)legitimisation strategies. These outcomes are in line with previous studies about mediated surveillance debates, which indicates that privacy attitudes transcend national boundaries. However, the inclusion of user-generated content adds an individual dimension to the existing body of research and reveals a personal perspective on surveillance issues.

KEYWORDS attitudes; framing; National Security Agency (NSA) revelations; privacy; public debates; surveillance

Introduction

"Because even if you're not doing anything wrong you're being watched and recorded" is Edward Snowden's answer to the question why people should care about surveillance (Rodriguez 2013). Snowden, a former National Security Agency (NSA) contractor, is responsible for leaking thousands of classified NSA documents to journalists. Information from these files is published in international newspapers, starting with *The Guardian* on June 6, 2013 (Greenwald 2013), revealing how the NSA collected incomprehensible amounts of data from millions of people worldwide. In the name of its foreign surveillance mission, the NSA collaborated with intelligence services, social networking sites, software developers, network providers and other parties to collect and monitor cell phone locations, contact lists, emails, conversations and other personal data (Angwin and Larson 2014). The NSA practices are a form of surveillance: the collection and processing of personal data for influencing or managing purposes (Lyon 2001).

Digital Journalism, 2017
Vol. 5, No. 3, 277–298, http://dx.doi.org/10.1080/21670811.2016.1234938

Unsurprisingly, the NSA revelations led to numerous news articles and public discussions. They also inspired academic scholars to reflect on the future of a post-Snowden cyberspace (Bajaj 2014), laws and regulations in a post-NSA era (Van der Sloot 2014), the NSA leaks' socio-technical consequences (Lyon 2014), the ethical implications (Lucas Jr 2014) and state-media–citizen relations (Digital Citizenship and Surveillance Society Project, http://www.dcssproject.net/). While the international press was captivated by the NSA revelations, reactions in Dutch newspapers seemed reassuring. "Most people are simply not interesting enough to be followed by the NSA" is a quote that frequently came up in Dutch news media (e.g. *De Volkskrant*, December 24, 2013). According to a newspaper article that discussed the impact of the NSA revelations in the Netherlands, Dutch citizens and politicians "don't care about espionage" (*Het Parool*, October 22, 2013). However, blogs and (tech) websites seemed to show more agitated reactions. People spoke out against a violation of privacy rights and were shocked by the role of national security agencies and commercial actors in the NSA surveillance of European citizens.

This article aims to provide an in-depth examination of Dutch privacy attitudes and viewpoints in public debates about the NSA revelations and to establish which sentiments prevail in professional news coverage as well as non-journalistic online contributions. The analysis and findings not only complement academic research about privacy attitudes and surveillance debates, but are also relevant for actors and organisations concerned with privacy issues and online civil rights.

The first theoretical section considers the definition of privacy as a social issue, analyses of surveillance media representations and the Dutch context of the public debate at hand. The subsequent methodological section covers an explanation of the data sample and the analysis, followed by a detailed description of the resulting frames and their connection to theoretical notions of privacy that address the societal and individual impacts of digital surveillance.

Background

Privacy as a Social Issue

Privacy is a complex concept that encompasses various views about human freedom, rights, personal values and information flows (Bennett 2011; Rosenzweig 2012). Building on one of the earliest notions of privacy that emphasised the right to be let alone (Warren and Brandeis 1890), legal scholars conceive of privacy as control-over-information and focus on personal information as property (see the critical review by Solove 2002). Philosophers take a different approach by exploring the boundaries between the public and the private and by addressing privacy as a personal value. On the one hand, they focus on controlling access to one's inner aspects and relate privacy to intimacy, trust and identity. In this view, privacy is a vital component of human interaction and relationships (Schoeman 1984). On the other hand, descriptive and normative forms of privacy concerning information control are considered (Tavani 2007). A critical perspective addresses the politics of privacy, focusing on the dominance of corporations and governments in a digital economy, characterised by an unequal division of power and data ownership (Allmer 2013; Fuchs 2012; Sandoval 2014). Technical scholars propose more fluid notions of privacy to adapt to new technological advances

(Finn, Wright, and Friedewald 2013), incorporating the role of both individual and institutional control and responsibilities (Whitley 2009). They stress that problems related to different types of privacy require customised solutions and configurations (Van der Ploeg 2005).

Because the implications of massive data collection transcend the individual level, this study focuses on a notion of privacy as a social issue as proposed by Margulis (2003), inspired by Regan (1995). Individual, societal and governmental interests in privacy are included in this broader social perspective which explores how privacy is societally important in three ways. First, there is a common or shared interest in privacy and in a right to privacy. Second, privacy is "a societal value because it supports and is supported by a democratic political system" (Margulis 2003, 249) and, third, privacy can be seen as a societal good that needs to be distributed equally by institutional, technological, governmental and market forces. Threats to privacy almost exclusively arise in relationships between the individual and private or governmental organisations, and take place in the public and societal realm (249). The NSA revelations are discussed in this public and societal realm where relations between individuals and governmental security institutions, as well as commercial organisations, are at stake.

In the current data-driven society wherein social and working life are mediated and mediatised to a large extent, threats to privacy have increased tremendously. A recent Pew survey showed that attitudes towards privacy can be complex. A year after the NSA leaks, many American citizens believed that online privacy became impossible and felt that they lost control over how personal information is collected. Yet, they are willing to trade off their personal data for access to free services (Madden et al. 2014).

Media Representations of Surveillance

The public debate at hand consists of public responses about privacy following Snowden's revelations of far-reaching surveillance practices. Media attention to surveillance technologies intensified in the last two decades (Barnard-Wills 2011), while it also became more critical (Finn and McCahill 2010; Hronesova, Caulfield, and Guasti 2014). Whereas both UK and Canadian newspaper coverage of the introduction of CCTV (closed-circuit television) was almost exclusively supportive of surveillance (Greenberg and Hier 2009; McCahill 2003), later studies show more variety in news discourses. Finn and McCahill's (2010) extensive analysis of the representation of surveilled individuals in UK newspapers reveals a central discursive theme based on the flexible binary opposition of "us" (law-abiding citizens) versus "them" (deviants and out-groups). This division determines the framing of "good" versus "bad" surveillance technologies. Barnard-Wills (2011) explains how the "us" and "them" binary is used in a positive evaluation of "appropriate" surveillance (protecting "us" from "them") opposed to negative "inappropriate" surveillance ("us" surveilled by "them"). These evaluations are closely related to a trade-off narrative of security/crime control versus civil liberties/privacy (Barnard-Wills 2011), which is also visible in UK newspaper coverage about CCTV and body scanners (Hronesova, Caulfield, and Guasti 2014).

However, media representations of the NSA revelations differ distinctly from preceding media coverage because they revolve around a variety of combined surveillance technologies used on an unprecedented scale. Branum and Charteris-Black (2015) show

that UK newspaper coverage about the NSA revelations is coloured by the newspapers' ideology, news values and audience considerations. However, like the aforementioned trade-off discourses, Lischka's (2015) large-scale analysis of UK television and radio news broadcasts (part of the Digital Citizenship and Surveillance Society Project), distinguishes terrorism versus privacy as the two major themes in a variety of news media. Legitimising and delegitimising strategies play an important role in UK news broadcasts (Lischka 2015). Legitimation strategies are also visible in Schulze's (2015) analysis of German politicians' public reactions to the NSA revelations wherein terrorism is offered as a justification of surveillance measures.

Existing studies about media representations of surveillance mainly focus on the United Kingdom. In light of the aforementioned analyses of media coverage of NSA revelations, this article explores the Dutch news coverage while also considering the online reactions of citizens. The next section provides historical and cultural context to the Dutch public debate.

Open Curtains

The Dutch public debate offers an interesting case study for the examination of privacy attitudes. History offers three explanations for a trusting, care-free attitude that might have led to an indifferent stance towards the NSA revelation. First, Dutch history is characterised by the development of an early democracy and a democratic corporatist media system. Moderate political views prevail in the public debate (Hallin and Mancini 2004). In this, the Dutch situation differs from the United Kingdom, where press opposed the use of identity cards after the Second World War (Agar 2001) and where the ubiquity of CCTV cameras led to recurring public debates (e.g. McCahill 2003). Second, Dutch citizens never experienced far-reaching state surveillance and therefore lack a public memory of totalitarian surveillance measures infringing personal freedom. This sharply contrasts with the German case, where reactions to the NSA revelations occurred against the historical backdrop of two succeeding dictatorships (Schulze 2015). Third, the Dutch are well-known for their open culture which is exemplified by their large windows with open curtains. According to Bolt (2008), Dutch citizens keep their curtains open either to assure their neighbours that they have nothing to hide or because they are not ashamed of their everyday lives. Simultaneously, the open curtains allow for a form of social and informal surveillance that citizens consent to and in which they participate to increase a sense of safety (Vera 1989). While (online) privacy arguably transcends the elementary choice of (not) hiding yourself, the relevance of this openness of Dutch culture also emerges from the analysis.

More recently, a Eurobarometer survey showed that Dutch respondents feel comfortable with disclosing personal information when they use online services and applications or obtain online products (TNS Opinion & Social 2015). For almost half (48 per cent) of Dutch respondents providing personal information is not a big issue, and the Dutch are among the least concerned European citizens when it comes to not having control over their personal data. In addition, while the Netherlands is among the three countries with the highest share of respondents who claim to have heard of Snowden's revelations, only 43 per cent of the respondents indicated that the NSA leaks negatively impacted their trust in the use of personal data (TNS Opinion & Social 2015).

These survey results, combined with an open culture, moderate political debates and history, imply that the Dutch are indifferent towards privacy issues. This empirical study anticipates more complex Dutch privacy attitudes and is therefore based on an explorative research method. The next section explains how an inductive frame analysis is combined with a descriptive quantitative analysis to distil distinct privacy attitudes.

Method

Sample

To enable a detailed overview of the attitudes about privacy in the Dutch public debate about Snowden's revelations, a twofold content analysis was designed. Attitudes about privacy were distilled in the first stage, whereas the second level of analysis allowed for the interpretation of the role and extent of the attitudes in the public debate. The research design includes an inductive frame analysis (phase 1) and a descriptive content analysis (phase 2) of reactions about the NSA revelations which were published or posted in the two weeks after the first revelations, June 6 to 20, 2013. The sample is based on the first two weeks of the public debate to enable an analysis of all retrievable initial responses to the revelations which are not yet influenced by external parties or events.

The research units are reactions to Snowden's revelations: written accounts of the NSA leaks which include meaningful text elements (words, sentiments, metaphors, opinions) about privacy. The sample consists of both professional/journalistic and user-generated/non-journalistic content. The former includes articles and blogs written by professional authors: journalists, editors and professional bloggers (connected to a company, organisation or association); whereas the latter is published or posted by bloggers (on a personal note), members of the audience (in letters to the editor, and comments or reactions to online content) and forum participants.

The sample was constructed by the use of two search strategies. First, the offline coverage was collected via LexisNexis using the query "NSA AND privacy" to search all Dutch news and to collect reactions published in quality newspapers (such as *NRC Handelsblad* and *De Volkskrant*), popular newspapers (such as *De Telegraaf* and *Algemeen Dagblad*), regional newspapers (such as *Limburgs Dagblad*) and wire service reports (such as *ANP*). Second, online reactions were gathered via a demarcated Google search for results that originated in The Netherlands and were written in Dutch (search query: "allintext: NSA AND privacy"). This part of the sample includes forum threads on websites like the youth-oriented *Fok forum.nl*, (news) articles and comments on tech websites such as *Tweakers.net*, personal blogs like *Rebelsehuisvrouw.nl*, corporate blog posts on sites like *greenhost.nl*, and blog posts and comments on popular blogs such as provocative *GeenStijl.nl*, progressive *Joop.nl* and its counterpart *The Post Online*.

All articles were filtered for privacy attitudes: text sections wherein authors describe privacy in relation to the NSA revelations. Irrelevant results were omitted to end up with a selection of responses that displayed one or more attitudes about privacy. The resulting sample (see Table 1) consists of 107 offline newspaper articles and 150 online contributions. The sample comprises 154 items from professional authors and 103 items that qualify as user-generated content. The data sample is highly diverse.

TABLE 1
Data sample

Content	Offline	Online	Total
Professional author	106	48	154
User-generated content	1	102	103
Total	107	150	257

For instance, news articles are often longer than forum threads, and blog authors take a more personal approach than news wire articles. However, this diversity does not hinder the comparability of results because the analysis focused on mapping privacy sentiments and actors in the public debate instead of comparing full articles.

Content Analysis

Attitudes about privacy were distilled via an inductive frame analysis, identifying recurring patterns in online/offline and professional/non-journalistic content. Frames are representations of a perceived reality wherein the selection and salience of aspects result in "a particular problem definition, causal interpretation, moral evaluation and/or treatment recommendation for the item described" (Entman 1993, 52). They can be regarded as "principles of selection, emphasis and presentation composed of little tacit theories about what exists, what happens, and what matters" (Gitlin [1980] 2003, 6).

A twofold inductive frame analysis was conducted (inspired by grounded theory; see, among others, Strauss and Corbin 1990; Van Gorp 2007). Inductive frame analysis enables the inclusion of general as well as more context-specific attitudes and viewpoints. The process contained three levels of analysis. First, all meaningful text elements were listed; these are the framing devices (Gamson and Modigliani 1989) which take the form of metaphors (e.g. "open curtains"), examples (e.g. "Echelon"), catchphrases (e.g. "Big Brother is watching you") or specific words (e.g. "safety"). Subsequently, the devices were clustered and supplemented with reasoning devices; explicit and implicit statements from the texts that address causes and consequences (Gamson and Modigliani 1989), such as "privacy is a farce". The resulting clusters were labelled in a frame matrix (see Table 2).

Subsequently, a descriptive content analysis was conducted to map the roles and the distribution of the resulting frames in the public debate. In total, 257 contributions were coded in SPSS, noting the author, origin and media type, listing all the actors that express an opinion about privacy and interpreting privacy attitudes according to the six frames that were distilled in the frame analysis. The coding process was guided by a codebook, which is included in Appendix A. Because coding for frames (in other words, deciding which specific frame is present in an article or online reaction) can be subject to interpretation, an intercoder reliability test was conducted for the frame-variable. The test resulted in a sufficient Krippendorff alpha score of 0.856 (Krippendorff 2004). For 27 items, the contribution proved to be too ambiguous or too short to decide on a frame.

TABLE 2
Frames that define an attitude towards privacy (inspired by Gamson and Lasch 1993 and Van Gorp 2007)

Frame	Problem definition	Cause	Consequences	Responsible for solution	Moral/emotional basis	Key concepts	Metaphors, choice of vocabulary
End justifies the means	100% privacy and 100% safety do not go together	Threat of terrorism	There is no option but to sacrifice a small amount of personal privacy for the safety of society	Governments/ security agencies.	Loss of privacy is a small sacrifice compared with the danger of terrorist attacks. Feelings of fear, trust in governments	Trust, Safety, Protection, Necessary, Terrorists, Safe society	A second 9/11, more than 50 terrorist attacks prevented, safety is the fundamental human right, surveillance is limited to metadata, give up an ounce of privacy for a kilo of safety
Nothing to hide	Privacy might not be possible online, but that is not a problem	Details get lost in the enormous pile of data that is collected	Privacy is not really threatened	There is no need for a solution	There is no need to panic. When you have got nothing to hide, you do not need to worry. Careless attitude	Uninteresting, Exaggerated, Normal citizens	If you've got nothing to hide there is nothing to fear, making efforts to hide, makes you suspicious, can't see the wood for the trees, open curtains-loving Netherlands, if I want a private conversation, I will meet in real-life
Privacy paradox	You cannot participate in online society if you do not give in your privacy	Online society is built on and driven by personal data	There will be no privacy left	Online services, users	Worries about privacy conflict with the benefits and convenience offered by online services. It is up to the user. Conflicting feelings	Convenience, Consent, Responsibility, Choice	Digitally/socially isolated, behaviour makes money, convenience over privacy, if you put your holiday photos online, you are to blame, own choice and responsibility, "free of charge" has its price

(*Continued*)

TABLE 2 (*Continued*)

Frame	Problem definition	Cause	Consequences	Responsible for solution	Moral/emotional basis	Key concepts	Metaphors, choice of vocabulary
Empower the user	If we want to protect our privacy, users need to be empowered	The importance of privacy has been neglected. An effective public debate about privacy is needed	If people remain uniformed, commercial firms and governments face no obstacles in their abuse of personal data	Users when it comes to privacy and governments need to design protective legislation	Privacy is a fundamental right, feelings of empowerment	Awareness, Transparency, Protecting, Control, Empowering	Importance of privacy, encryption, reclaim your data, open source, decide what others can find about you, privacy is in your own hands, lock on bathroom door
Privacy is dead	The NSA revelations prove once again that online privacy ceased to exist a long time ago	Governments have been collecting personal data for years	The effectivity of government's research methods has increased enormously	There is no solution	If you want to be somewhat safe, you need to get off the internet, feelings of disillusionment	Echelon, Lost battle, Unsurprisingly	Golden age of privacy is over, PRISM: old wine in new bottles, AIVD and MIVD [Dutch Intelligence and Security Services] infiltrate computers since 2002, fun while it lasted, newsflash, privacy is a farce, privacy existed in a distant past
Orwellian dystopia	Privacy is in danger because far-reaching digital control created an Orwellian surveillance society	Governments granted themselves too many rights	Computer-controlled surveillance will harm innocent citizens, therefore needs to be restricted	A different type of government	Mass surveillance makes citizens into suspects, extremely vulnerable to false allegations and future leaders with questionable political agendas, feelings of distrust in governments	Dystopian, Orwellian, Undemocratic, Big Brother	Right to privacy, Thought Police, there will be no place to hide, United Stasi of America, Big government is watching you, safety implies privacy, Turnkey tyranny, terrorism used as a pretext, securocrats

Results

Six Frames

The inductive frame analysis resulted in six distinct frames. The descriptive content analysis mapped the online and offline recurrence and use of these frames by professional and non-journalistic contributors to the Dutch public debate about the NSA revelations.

The Dutch public debate appears (far) less indifferent than expected, since the *nothing to hide*-frame is visible in only 7 per cent of all contributions (see Table 3). In contrast, the most salient frame is the activist attitude (22 per cent) which aims to *empower the user* and strives for the protection of privacy as a fundamental right. Two other, fundamentally opposed frames also play an important role. The *end justifies the means*-frame (18 per cent) supports the intentions of governments to protect citizens and is willing to trade off privacy to ensure a safe society. This frame sharply contrasts with the *Orwellian dystopia*-frame (20 per cent) that stresses the negative consequences of surveillance and foresees a dark future wherein privacy is non-existent and everyone is guilty until proven innocent. The defeatist *privacy is dead*-frame (18 per cent) contains a history of a long lost trust in privacy and is mainly voiced online. The two most pessimistic frames are more often found online than offline (see Table 3) and more often in user-generated content than in professional reactions (see Table 4). A personal struggle for privacy is reflected in the *privacy paradox*-frame which plays a minor role in the public debate about the NSA revelations. Before the six frames are discussed in detail, the temporal development of the debate will be addressed (see Figure 1).

Dutch reactions to the NSA revelations kick-started on 7 June 2013, reaching a second peak on 10 and 11 June. These two peaks are related to meaningful events; the first peak is connected to the first NSA revelations about Verizon and PRISM (a surveillance programme that collects personal information via communication platforms and services), whereas the second peak links to the disclosure of Snowden's identity on 10 June. After the second peak, the Dutch debate became more diverse. Instead of focusing on the same subject, newspapers published background information about various topics (such as the political consequences, Edward Snowden's identity and the situation in Europe). A wide range of opinions is voiced in columns, opinion pieces, responses of the public and (personal) blogs.

The first day of the debate contained the most coverage; a total of 66 (online and offline) contributions which mainly focused on the NSA collecting Verizon phone

TABLE 3
Distribution of frames over all reactions

	End justifies the means	Nothing to hide	Privacy paradox	Empower the user	Privacy is dead	Orwellian dystopia	No distinct frame	Total
Offline	26 (24)	3 (3)	4 (4)	28 (26)	15 (14)	11 (10)	20 (19)	107 (100)
Online	20 (13)	16 (11)	7 (5)	29 (19)	32 (21)	39 (26)	7 (5)	150 (100)
Total	46 (18)	19 (7)	11 (4)	57 (22)	47 (18)	50 (20)	27 (11)	257 (100)

$N = 257$. Percentages are given in parentheses.

TABLE 4
Distribution of frames over professional and user-generated content (UGC)

	End justifies the means	Nothing to hide	Privacy paradox	Empower the user	Privacy is dead	Orwellian dystopia	No distinct frame	Total
Professional	31 (20)	3 (2)	7 (5)	47 (30)	21 (14)	19 (12)	26 (17)	154 (100)
UGC	15 (15)	16 (15)	4 (4)	10 (10)	26 (25)	31 (30)	1 (1)	103 (100)
Total	46 (18)	19 (7)	11 (4)	57 (22)	47 (18)	50 (20)	27 (11)	257 (100)

N = 257. Percentages are given in parentheses.

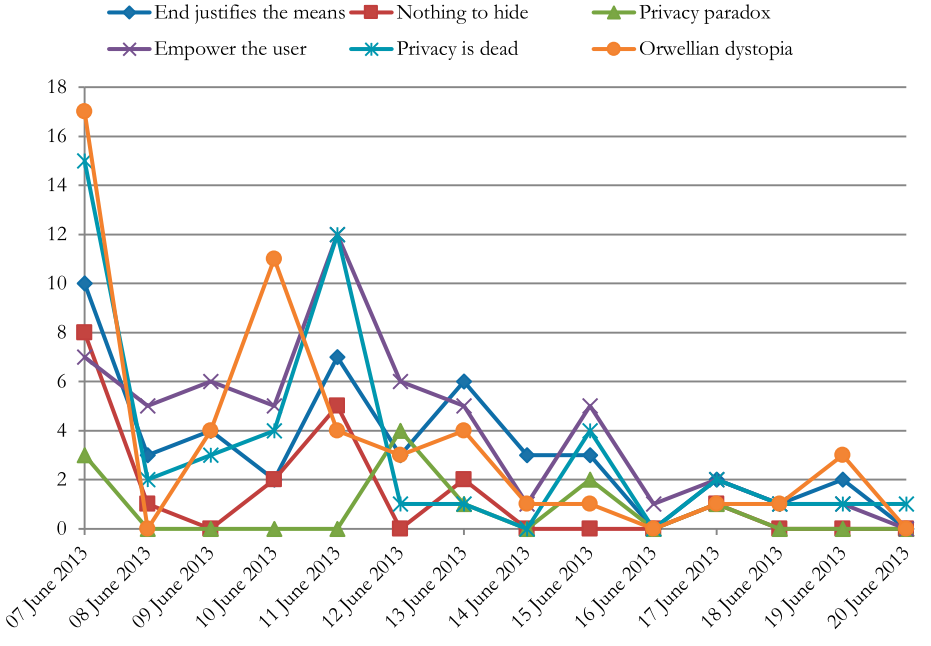

FIGURE 1
Development of frames over time

records and PRISM. According to US government officials, PRISM targets foreign nationals. It is therefore not surprising that the *end justifies the means*-frame is visible in 10 out of 66 reactions as it often cites authority figures who defend the need for the surveillance measures. However, strikingly, the most often recurring attitudes on that day are reflected in the *privacy is dead*-frame (15/66) and the *Orwellian dystopia*-frame (17/66). The most pessimistic attitudes were voiced directly after the first revelations, which indicates that the debate started off in a heated manner. Less emotional is the *empower the user*-frame that offers background information about how citizens should protect their privacy (7/66). This frame is opposed by the *nothing to hide*-frame (7/66) that downplays the consequences of digital surveillance.

The second peak in the debate mainly discusses the disclosure of Snowden's identity and includes 64 reactions in two days (10 and 11 June). Again, the *privacy is dead*-frame (16/64) and the *Orwellian dystopia*-frame (15/64) play a large role in this

section of the debate. However, the *empower the user*-frame (17/64) has the strongest presence, describing how Snowden stresses the importance of a public debate about privacy and encouraging the user to care about their privacy. The other frames do not address the impact of Snowden's revelation on the privacy of citizens. Instead, the *end justifies the means*-frame is visible in 9/64 contributions and emphasises the risks of Snowden's revelations for the safety of society, whereas the *nothing to hide*-frame (7/64) disregards the impact and importance of Snowden's revelations in general. The *privacy paradox*-frame plays a small role in the debate as it only occurs in 4 per cent of the reactions. In the next section, the six frames are described in detail.

End Justifies the Means: "Give Up an Ounce of Privacy for a Kilo of Safety"

The notion that the end justifies the means is the basis of the first frame that is visible in 18 per cent of all reactions and is almost evenly divided between offline and online content. The "end" refers to public safety that is threatened by terrorism. In order to protect the safety of society, there is no option but to sacrifice a small amount of personal privacy (the means). Key words of this frame are "public interest", "safe society", "necessary", "safety", "trust", "protection" and "terrorism". According to voices in this frame, the most fundamental human right is safety. The problem definition of this frame is based on the legitimisation of NSA surveillance by authority figures such as US president Barack Obama and NSA directors Keith Alexander and James Clapper. Obama claimed that he strives for a balance, because "100 per cent safety and 100 per cent privacy are incompatible". Alexander stated that more than 50 terrorist attacks were prevented in 20 countries to prove that NSA surveillance leads to a safer society. Safety is presented as the responsibility of citizens, who risk it if they want to protect their privacy. A Dutch politician literally asked people to: "give up your privacy for a safe society" (*Security.nl*, June 6).

In addition to stressing horrible events that (could) have been prevented and that legitimise the use of surveillance measures, authority figures and security agencies trivialise the impact of surveillance. They claim that only metadata is collected, instead of the content of phone calls and other communication. Obama's statement "nobody listens to your phone calls" is often repeated in Dutch newspapers (e.g. *NRC Next*, June 11, 2013). The Dutch minister of Justice stressed that the use of surveillance techniques "keeps an eye on the personal sphere" and that surveillance measures are taken "carefully, proportionately and effectively" (*ANP*, June 11).

Trust in government forms the basis of the *end justifies the means*-frame. One-third (33 per cent) of all the reactions that display this frame consists of user-generated content. This often concerns anxious Dutch citizens who fear terrorism and are willing to "give up an ounce of privacy for a kilo of safety". Two-thirds (67 per cent) of the reactions that contain this frame are written by professional authors, mainly in newspapers. This can be explained by the newsworthiness of authority figures in general, and the crucial role of Barack Obama, Keith Alexander and James Clapper in the events. While most journalists only quote authority figures, some actively support this frame. An example is an opinionated news article wherein the author claims: "Our safety is ensured [by the NSA]. What is more important: security or privacy?" (*Trouw*, June 14, 2013).

The anxious attitude that strives for a balance between privacy and safety relates closely to Gellman's (2002) argument that privacy is not a singular trait because people can never be in complete control of their personal information. Privacy will always be a complex value-laden concept and it is all about "cutting up the privacy pie" (256). However, it is crucial to strike a balance between safety and privacy by means of legislation and to address the consequences of laws that affect privacy (Gellman 2002). Gellman's ideas are clearly reflected in the manner in which the *end justifies the means*-frame cites authority figures who justify the surveillance measures as they focus on the positive consequences of the measures for public safety. In the other frames, various other voices oppose this viewpoint and address the negative consequences of surveillance measures as they fear for a loss of personal freedom and privacy. However, the next frame is based on the claim that the surveillance measures have no negative consequences for law-abiding citizens.

Nothing to Hide: "If You Are Not Doing Anything Wrong, You Have Nothing to Fear"

The second frame is based on the recurring statement "I've got nothing to hide". People state that they are not interesting enough to be followed by the NSA. This frame is visible in only 7 per cent of all reactions. The finding that this frame is less salient in the public debate may well be caused by the fact that those who are not concerned or indifferent about privacy are per definition less likely to engage in public privacy debates.

An open Dutch culture is described in this frame, whereby open curtains are discussed as the offline example of the manner in which Dutch people refuse to care about other people watching their lives. This frame is almost exclusively manifest online in user-generated content. Key words like "uninteresting", "exaggerated" and "normal citizens" are frequently used. This narrative offers a binary division and separates "ordinary civilians" from "people who have something to hide". The former category has no need for panic because they are not doing anything wrong. An online reaction to a news article on a tech website states "I'm not a criminal and therefore I don't expect to appear on the government radar" (*Tweakers.net*, June 14, 2013).

In addition, a blog author claims that internet users do not have to fear the mass surveillance because "the incredible amount of information collected will most definitely lead to an information overload" (*42bis.nl*, June 13, 2013). Online privacy may be non-existent, but that is not a problem because personal details are impossible to track in the enormous pile of data collected by the NSA. People claim that their holiday pictures, their everyday life updates and their online preference are uninteresting to the NSA; "They will not even be interested in your secretly stored naughty pictures" (*Joop.nl*, June 7, 2013). Therefore, according to contributions displaying this frame, there is no need for a solution and a careless attitude can be upheld.

According to Solove (2008), this attitude is based on a *narrow understanding of privacy* which does not value privacy highly. This attitude focuses on very limited disclosure of particular information that is not likely to be threatening to the privacy of law-abiding citizens. The *nothing to hide*-argument suggests that only people who are engaged in or who desire to conceal unlawful activities should be concerned. Solove (2008) argues that this account of privacy is problematic because it fails to include

"non-discreditable information about people that they nevertheless want to conceal because they find it embarrassing or just do not want others to know about" (Solove 2008, 752). Solove maintains that the *nothing to hide*-argument is problematic because it is based on the assumption that privacy is about hiding bad things, while the capabilities of the current state of surveillance transcend the level of uncovering hidden information. The opaque and unaccountable process of surveillance combines all different types of (meta)data not only to collect information that "we might really want to conceal", but also to predict future behaviour (Solove 2008, 766). The lack of transparency disables a proper basis for the *nothing to hide*-frame because it is impossible to have full comprehension of what one is hiding for which purposes.

Privacy Paradox: "We Prefer Convenience Over Privacy"

Actors in the third *privacy paradox*-frame are aware of the problematic consequences of surveillance. Whereas the previous frames did not regard the impact of surveillance as a real threat to privacy, voices in this frame express more concern. The *privacy paradox* attitude plays a minor role in the debate compared to the other frames. It is visible in only 11 contributions (4 per cent of the sample), which are evenly divided between online and offline reactions and between professional and user-generated sources. Key words in this frame are "convenience", "consent", "responsibility" and "choice". Facebook and Google are often mentioned as companies that are pretending to be free of charge while users pay with personal data. Authors of this frame state that online society is built on and driven by personal data. This closely relates to Campbell and Carlson's (2002) notion of the *commodification of privacy*; a process rendering privacy concerns as consumer burdens. Concerns are a hindrance because they conflict with the user agreements of popular services such as Facebook, Google Maps and WhatsApp, which offer users convenience and social and functional benefits. As the author of a blog states: "Google is spying on us—with our permission. You can oppose this, but no one forces you to use this service" (*Kennisland.nl*, June 13, 2013). Citizens experience a paradoxical discrepancy between privacy concerns and online behaviour. This discrepancy is referred to as the *privacy paradox* (Barnes 2006; Potzsch 2009). The privacy paradox describes a tension between users' awareness of privacy concerns and their online behaviour.

As a result of this tension, actors within the third frame express the fear of being digitally and socially isolated. A blog post states: "users have to choose between giving up their privacy or ending up in social isolation" (*Tweetsmania.nl*, June 12, 2013). When they decide to avoid services that require personal information, they will miss out on social updates and events and functional tools that make their lives more convenient. Privacy is seen as a personal choice, a personal responsibility and a personal burden. As the author of a critical blog post puts it: "If you choose convenience over privacy and decide to put your summer snapshots online, you are to blame when they fall into the wrong hands" (*Daskapital.nl*, June 9, 2013).

Empower the User: "Privacy is in Your Own Hands"

The fourth frame also regards privacy as a personal responsibility of users. This frame is the most often recurring frame in contributions to the public debate about

the NSA revelations, and is mainly used by professional authors. It is almost evenly distributed between online and offline reactions. Academic privacy experts are almost as often cited as organisations that defend online civil rights (e.g. Bits of Freedom and European Electric Frontiers). US, EU and Dutch authority figures also play an important role in this frame as they demand better legislation and agreements about privacy. In the United States, senators Mark Udall and Ron Wyden stated that they were shocked about the current state of privacy (*Trouw*, June 8, 2013), (former) EU commissioner Neelie Kroes wanted to protect privacy "as a fundamental human right" (*ANP*, June 10, 2013), and a Dutch socialist politician demanded more transparency (*NRC Next*, June 14, 2013). In addition to the political outcry, this frame emphasises that the importance of privacy is neglected in the public debate about the NSA revelations. "Awareness", "transparency", "protection", "control" and "empowering" are key words in this frame. Actors advocate more transparency when it comes to the use of personal data by governments and companies and strive to create awareness about privacy. A blog post states: "Everyone is entitled to digital transparency. The right to decide what you share and who can use your data" (*Twittermania.nl*, June 12, 2013).

According to voices in the *empower the user*-frame, citizens need to be empowered and must be handed the possibility to exercise control over their own data and privacy by means of protection. Authors take a practical approach as reactions that display this frame often offer advice on how to protect personal privacy, discussing the possibilities of encryption, open source software and other digital tools. This frame is grounded by a notion of self-determination, described by Debatin (2011) as a moral principle that enables individuals to control access to their private sphere and to regulate the flow and context of their information. The notion of self-determination is closely linked to the idea of privacy as contextual integrity defined by Nissenbaum (2010, 127) as a right to an "appropriate flow of personal information" which is determined by the context wherein personal data are distributed. The notion of context is influenced by roles, activities, norms and values, and the characteristics of different contexts are crucial in establishing privacy violations. Consequently, norms of appropriateness are socially constructed (127).

While the *empower the user*-frame addresses the potential threat of surveillance, it is optimistic about privacy in general. Appropriate tools, protection and legislation can potentially restore the endangered state of privacy. A hopeful attitude foresees a future wherein users can control (commercial and surveillance actors having) access to their data, in order for them to establish an appropriate flow and context for their personal information. However, on a more critical note, it can be problematic to shift all responsibilities to citizens who do not possess the proper means or knowledge to protect their privacy. This concern was also voiced in a reaction to a blog: "privacy is in your own hands, which is, in fact, the biggest problem" (*Geenstijl.nl*, June 9, 2013).

Privacy is Dead: "If You Want to Be Somewhat Safe, You Need to Leave the Internet"

The hopeful attitude of the fourth frame is hard to find in the fifth frame. According to authors of this frame, there is no hope for improvement of the miserable state of privacy, and no hope for a future without digital surveillance. "The only way to be

safe and to maintain your privacy is to leave the digital realm" is stated in a reaction to an article on a tech website (*Onemorething.nl*, June 7, 2013). Whereas actors of the previous frame believe in the future of privacy, this frame lacks optimism. The *privacy is dead*-frame displays disillusionment and is mainly voiced online. The most important actor in this frame is Edward Snowden, as he proved once again that online privacy ceased to exist. The frame is primarily visible on tech blogs and tech websites (e.g. *Tweakers*, *IT Pro*, *Bright*). Tech blogs are considered to be important influencers of the public and industry attitudes towards digital technologies. They often display internet centrism; a specific focus on the internet as "a powerful or indispensable tool within a given social context" (Freelon, Merrit, and Jaymes 2015, 176). In this frame, the internet is seen as powerful to such a large extent that its power marked its own demise. This attitude can be described as an example of digital defeatism which, according to Mozorov (2013), occurs when people dismiss the internet as a lost cause and give up on it. Technology is seen as uncontrollable and there is nothing that humans can do to prevent the decay of online freedom. The apt title of a newspaper article states: "Internet: Fun While it Lasted" (*NRC*, June 12, 2013).

In this frame, the loss of the promises of the internet is mourned, and contributions on tech blogs and websites offer no solutions. The battle for privacy and online freedom was lost long ago, when the existence of Echelon came to light (a mass surveillance system of the United States and United Kingdom which monitored phone calls, fax traffic and emails). Actors in this frame are not surprised by the NSA revelations and mock people who express shock, such as a blog post that states: "This cannot come as a surprise. We stood by and watched it happen" (*Grenswetenschap.nl*, June 11, 2013).

Orwellian Dystopia: "Big Government is Watching You"

Whereas actors in the fifth frame have lost all hope in the future of privacy, authors within this sixth frame are disheartened to such a large extent that only fear for a pitch-black future is left. Authors argue that Snowden's revelations proved that the surveillance society described in George Orwell's *1984* became reality. A reaction to a tech article claims that the current situation is even worse: "Modern governments are even smarter than Orwell foresaw: they let people bring their own 'telescreens' into their houses. And not only that, they even let them publish everything about their lives" (*tweakers.net*, June 7, 2013).

Visible in 20 per cent of all reactions, this frame conveys the deepest worries of actors in the Dutch debate about the NSA revelations. Surveillance measures are described as "dystopian", "tyrannical", "draconic" and "undemocratic". The frame is voiced in opinionated newspaper content, but is mainly visible in online reactions and in user-generated content. Authors in this frame often refer to Snowden's most pessimistic statements, including his fear for "turn-key tyranny" (*ftm.nl*, June 10, 2013): the possibility of tyranny activated by the turn of a key, enabled by state-of-the art surveillance measures. A tech company states on their corporate blog: "We believe that the use of uncontrolled, undemocratic and unlimited control mechanisms is more likely to create a less safe world than a safer one" (*greenhost.nl*, June 11, 2013).

Unsurprisingly, this frame shows a deep distrust in governments and political systems that allegedly granted themselves too many rights. Metaphorical statements such

as "Big Government is watching you", "The United Stasi of America" and "Big Brother" are often used. Authors fear that surveillance practices regard citizens as guilty until proven innocent. Consequentially, mass surveillance makes citizens extremely vulnerable to false allegations and future leaders with questionable political agendas. The fear expressed in this frame is supported by Mayer-Schönberger and Cukier's (2013) concerns about the risk of falling victim to a dictatorship of data, which abuses personal data as a source of repression. The only possible solution is a different type of government that restricts digitally controlled surveillance.

Conclusion

The aftermath of the NSA revelations led to international debates about privacy and surveillance. This study examined a public debate about the Snowden leaks in the Netherlands to uncover Dutch attitudes about privacy. The resulting six frames reveal a variety of privacy attitudes ranging from untroubled and hopeful to deeply pessimistic sentiments. Dutch attitudes towards privacy are thus far more diverse than suggested by the newspapers and survey results cited earlier in this article, which mainly highlight an indifferent stance. This indicates that the inclusive approach of this article, with a focus on a great variety of sources and responses, led to a more comprehensive overview of Dutch privacy attitudes.

The most often used frame displays hope for a future wherein citizens are able to control (access to) their personal data online. While this is a positive basis, the debate fails to pay attention to regulations to protect citizen rights. Only the *empower the user*-frame mentions politicians who stress the need for regulations, but they seem to be overshadowed by (prominent) authority figures that condone safety measures and actors stressing that citizens are responsible for safeguarding their personal data. When citizens are held accountable for their privacy (instead of government institutions and commercial actors), privacy is perceived as a personal instead of a social issue. This is problematic because citizens do not have the means to protect their privacy fully.

The findings are in line with previous studies about the media representation of surveillance. First, the *nothing to hide*-frame offers a clear distinction between law-abiding citizens and people who have something to hide. The authors making this distinction place themselves in the first category, which reflects the binary distinction between "us" and "them" as described by Finn and McCahill (2010). Second, the trade-off between privacy/personal liberties and safety/security as found in UK media representations about surveillance technologies (Barnard-Wills 2011; Hronesova, Caulfield, and Guasti 2014) and the NSA revelations (Lischka 2015), is to be found in multiple frames. Voices reflect on this trade-off in the *end justifies the means*-frame whereby safety is chosen over privacy, whereas voices in the *Orwellian dystopia*-frame highlight the risks of governments making this decision for their citizens. The *privacy paradox*-frame introduces yet another trade-off between privacy and convenience. Finally, targeting the frame analysis towards causes and consequences revealed how different actors (de)legitimise surveillance measures, as was also found in other recent studies (Lischka 2015; Schulze 2015). In the *end justifies the means*-frame, US government officials legitimise surveillance in a war against terror narrative, whereas citizens and journalists in the *privacy is dead*-frame delegitimise surveillance by emphasising the

negative consequences. Not only the actions of governmental actors are (de)legitimised in the resulting frames, they also offer insight in the legitimisation of citizens' behaviour. For instance, the *nothing to hide*-frame legitimises the use of online media and the *privacy paradox*-frame (partly) legitimises the preference of convenience over privacy.

The similarities in the outcomes of this study and previous analyses of surveillance debates show that the use of binary "us" versus "them" divisions, a trade-off narrative and (de)legitimising strategies transcend national spheres. It would be worthwhile to study whether these constructions and logics are also evident in other countries, in and outside Europe. The use of an inductive frame analysis, the focus on privacy and the inclusion of user-generated content allowed for the construction of an inclusive and contextual account of a surveillance debate. The research findings move beyond the reach of previous studies because personal legitimatisation strategies were revealed, a perspective often neglected in studying news coverage. The analysis of user-generated content is highly recommended for future research because it broadens the scope of news coverage analysis to a more comprehensive account of public debates that also involves non-journalistic actors.

A limitation of this research is the scope of the data collection. The study aims to offer a comprehensive overview of the public debate following the NSA revelations, but, because of feasibility and availability constraints, the analysis remains limited to text. To investigate further the public debate, television and radio debates could be examined to observe whether they convey different attitudes about privacy. In addition, the sampling period of two weeks is relatively short. It would be interesting to contrast the current findings cross-temporally with mentions of the NSA revelations in later debates about privacy or surveillance, to see how (the tone of) these debates and particular privacy frames and attitudes mature or change over time, also in connection with other major "events" related to privacy (e.g. other scandals, new legislation). Furthermore, additional research is needed, which compares privacy debates about other issues to assess how the construction of privacy attitudes is impacted by domain-specific factors (e.g. online commerce versus public safety) as well as national differences, e.g. in media systems (Hallin and Mancini 2004) or cultural values (e.g. Cecere, Le Guel, and Soulié 2015). This way, contextual differences in privacy debates can be identified, in order to contribute to a broader and even more in-depth understanding of public notions of privacy.

DISCLOSURE STATEMENT

No potential conflict of interest was reported by the authors.

REFERENCES

Agar, Jon. 2001. "Modern Horrors: British Identity and Identity Cards." In *Documenting Individual Identity: The Development of State Practices in the Modern World*, edited by Jane Caplan and John C. Torpey, 103–120. Princeton: Princeton University Press.

Allmer, Thomas. 2013. "Critical Internet Privacy Studies." *Fast Capitalism* 10 (1). https://www.uta.edu/huma/agger/fastcapitalism/10_1/allmer10_1.html.

Angwin, Julia, and Jeff Larson. 2014. "The NSA Revelations All in One Chart." *Pro Republica*. June 30. https://projects.propublica.org/nsa-grid/

Bajaj, Kamlesh. 2014. "Cyberspace: Post-Snowden." *Strategic Analysis* 38 (4): 582–587.

Barnard-Wills, David. 2011. "UK News Media Discourses of Surveillance." *The Sociological Quarterly* 52 (4): 548–567.

Barnes, Susan B. 2006. "A Privacy Paradox: Social Networking in the United States". *First Monday* 11 (9). http://firstmonday.org/ojs/index.php/fm/article/viewArticle/1394.

Bennett, Colin J. 2011. "In Defence of Privacy: The Concept and the Regime." *Surveillance & Society* 8 (4): 485–496.

Bolt, Rodney. 2008. *Xenophobe's Guide to the Dutch*. London: Oval Books.

Branum, Jens, and Jonathan Charteris-Black. 2015. "The Edward Snowden Affair: A Corpus Study of the British Press." *Discourse & Communication* 9 (2): 199–220.

Campbell, John Edward, and Matt Carlson. 2002. "Panopticon.Com: Online Surveillance and the Commodification of Privacy." *Journal of Broadcasting & Electronic Media* 46 (4): 586–606.

Cecere, Grazia, Fabrice Le Guel, and Nicolas Soulié. 2015. "Perceived Internet Privacy Concerns on Social Networks in Europe." *Technological Forecasting & Social Change* 96: 277–287.

Debatin, Bernard. 2011. "Ethics, Privacy, and Self-Restraint in Social Networking." In *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*, edited by Sabine Trepte and Leonard Reinecke, 47–60. Berlin: Springer.

Entman, Robert M.. 1993. "Framing: Toward Clarification of a Fractured Paradigm." *Journal of Communications* 43 (4): 51–58.

Finn, Rachel, and Michael McCahill. 2010. "Representing the Surveilled: Media Representations and Political Discourse in Three UK Newspapers." *Political Studies Association Conference Proceedings*. Accessed July 8, 2016. https://www.researchgate.net/profile/Rachel_Finn/publication/242715854_'Representing_the_Surveilled_Media_Representation_and_Political_Discourse_in_Three_UK_Newspapers/links/0c96052e8bf6d0285f000000.pdf

Finn, Rachel, David Wright, and Michael Friedewald. 2013. "Seven Types of Privacy". In *European Data Protection: Coming of Age*, edited by Serge Gutwirth, Ronald Leenes, Paul de Hert and Yves Poullet, 3–32. Dordrecht: Springer Netherlands.

Freelon, Deen, Sarah Merrit, and Taylor Jaymes. 2015. "Focus on the Tech." *Digital Journalism* 3 (2): 175–191.

Fuchs, Christian. 2012. "The Political Economy of Privacy on Facebook." *Television & New Media* 13 (2): 139–159.

Gamson, William A., and Kathryn Eilene Lasch. 1983. "The Political Culture of Social Welfare Policy". In *Evaluating the Welfare State. Social and Political Perspectives*, edited by Shimon E. Spiro, and Ephraim Yuchtman-Yaar, 397–415. New York: Academic Press.

Gamson, Willam A., and Andre Modigliani. 1989. "Media Discourse and Public Opinion on Nuclear Power: A Constructionist Approach." *American Journal of Sociology* 95 (1): 1–37.

Gellman, Robert. 2002. "Perspectives on Privacy and Terrorism: All is Not Lost—Yet." *Government Information Quarterly* 19: 255–264.

Gitlin, Todd. (1980) 2003. *The Whole World is Watching: Mass Media in the Making & Unmaking of the New Left*. Berkeley: University of California Press.

Greenberg, Josh, and Sean Hier. 2009. "CCTV Surveillance and the Poverty of Media Discourse: A Content Analysis of Canadian Newspaper Coverage." *Canadian Journal of Communication* 34: 461–486.

Greenwald, Glenn. 2013. "NSA Collecting Phone Records of Millions of Verizon Customers Daily." *The Guardian*. June 6. http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

Hallin, Daniel C., and Paulo Mancini. 2004. *Comparing Media Systems: Three Models of Media and Politics*. Cambridge: Cambridge University Press.

Hronesova, Jessie, Tristan Caulfield, and Petra Guasti. 2014. "The Xanadu of Surveillance: Report on Security Perceptions in the British Online Media." *Seconomics* (Discussion paper). http://www.seconomicsproject.eu/sites/default/files/content-files/downloads/the_xanadu_of_surveillance-uk.pdf.

Krippendorff, Klaus H. 2004. *Content Analysis. an Introduction to Its Methodology*. Thousand Oaks, CA: Sage.

Lischka, Juliane. 2015. "Surveillance Discourse in UK Broadcasting since the Snowdenrevelations". *Digital Citizenship and Surveillance Society Media Stream*. (Discussion paper). http://www.dcssproject.net/files/2015/12/DCSS_Broadcasting-report.pdf

Lucas Jr, George R.. 2014. "NSA Management Directive #424: Secrecy and Privacy in the Aftermath of Edward Snowden." *Ethics & International Affairs* 28 (1): 29–38.

Lyon, David. 2001. *Surveillance Society: Monitoring Everyday Life*. Berkshire: Open University Press.

Lyon, David. 2014. "Surveillance, Snowden and Big Data: Capacities, Consequences, Critique." *Big Data & Society* 1 (2): 1–13.

Madden, Marie, Lee Rainie, Kathryn Zickuhr, Maeve Duggan, and Aaron Smith. 2014. "Public Perceptions of Privacy and Security in the Post-Snowden Era." *Pew Research Center*. http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.p

Margulis, Stephen T. 2003. "Privacy as a Social Issue and Behavioral Concept." *Journal of Social Issues* 59 (2): 243–261.

Mayer-Schönberger, Viktor, and Kenneth Cukier. 2013. *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. New York: Houghton Mifflin Harcourt.

McCahill, Michael. 2003. "Media Representations of Visual Surveillance." In *Criminal Visions: Media Representations of Crime and Justice*, edited by Paul Mason, 192–213. Devon: Willan Publishing.

Mozorov, Evgeny. 2013. *To save Everything, Click Here: Technology, Solutionism, and the Urge to Fix Problems That Don't Exist*. London: Penguin.

Nissenbaum, Helen. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford UP.

Potzsch, Stefanie. 2009. "Privacy Awareness: A Means to Solve the Privacy Paradox? The Future of Identity in the Information Society." *IFIP Advances in Information and Communication Technology* 298: 226–236.

Regan, Priscilla M. 1995. *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill, NC: University of North Carolina Press.

Rodriguez, Gabriel. 2013. "Edward Snowden Interview Transcript FULL TEXT." *Policy.Mic*, June 9. http://mic.com/articles/47355/edward-snowden-interview-transcript-full-text-read-the-guardian-s-entire-interview-with-the-man-who-leaked-prism.

Rosenzweig, Paul. 2012. "Whither Privacy?" *Surveillance & Society*, 10 (3/4): 348–350.

Sandoval, Marisol. 2014. "Social Media? The Unsocial Character of Capitalist Media". In *Critique, Social Media and the Information Society*, edited by Christian Fuchs and Marisol Sandoval, 125–143. New York: Routlegde.

Schoeman, Ferdinand. 1984. "Privacy: Philosophical Dimensions." *American Philosophical Quarterly* 21 (3): 199–213.

Schulze, Matthias. 2015. "Patterns of Surveillance Legitimization: The German Discourse on the NSA Scandal." *Surveillance & Society* 13 (2): 197–217.

Solove, Daniel J. 2002. "Conceptualizing Privacy." *California Law Review* 90 (4): 1088–1155.

Solove, Daniel J. 2008. "I've Got Nothing to Hide and Other Misunderstandings of Privacy." *San Diego Law Review* 44: 745–772.

Strauss, Anselm, and Juliet Corbin. 1990. *Qualitative Data Analysis*. Beverly Hills: Sage.

Tavani, Herman T. 2007. *Philosophical Theories of Privacy. Methaphilosophy*, 31 (1): 1–22.

TNS Opinion & Social. 2015. "Special Eurobarometer 431 Data Protection." (report). http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf.

Van der Ploeg, Irma. 2005. *The Machine-Readable Body*. Shaker: Essays on Biometrics and the Informatization of the Body. Maastricht.

Van der Sloot, Bart. 2014. "Privacy in the Post-NSA Era: Time for a Fundamental Revision?" *JIPITEC*, 5 (2): 2–11. http://www.ivir.nl/publicaties/download/1437.

Van Gorp, Baldwin. 2007. "The Constructionist Approach to Framing: Bringing Culture Back in." *Journal of Communication* 57 (1): 60–78.

Vera, Hernan. 1989. "On Dutch Windows." *Qualitative Sociology*, 12 (2): 215–236.

Warren, Samuel D., and Louis. D. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review*, 4 (5). http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm.

Whitley, Edgar A. 2009. "Informational Privacy, Consent and the 'Control' of Personal Data." *Information Security Technical Report* 14 (3): 154–159.

Anouk Mols (author to whom correspondence should be addressed), Department of Media & Communication, Erasmus School of History, Culture and Communication, Erasmus University Rotterdam, The Netherlands E-mail: mols@eshcc.eur.nl

Susanne Janssen, Department of Media & Communication, Erasmus School of History, Culture and Communication, Erasmus University Rotterdam, The Netherlands E-mail: s.janssen@eshcc.eur.nl

Appendix A

Codebook Quantitative Analysis

	Name	Codes
01	Identification number	1–…
02	Date	mm.dd.yyyy
03	Title of source	...title...
04	Title of article	...title...
05	Author	...name...
06	Type of author (professional authors in italics—grouped during analysis)	0 = *Journalist* 1 = *Press agency* 2 = *Professional blogger (connected to company or organisation)* 3 = Blogger (on personal title) 4 = *Offline newsroom editors (redaction)* 5 = *Online newsroom editors (redaction)* 6 = Member of the audience 7 = Forum participant 8 = *US journalist* 97 = Other 99 = Unknown
07	Source	0 = Offline 1 = Online
08	Media type	0 = Newspaper 1 = Press agency publication 2 = News magazine 3 = Weblog 4 = Internet forum 5 = News website 6 = Tech website 97 = Other 99 = Unknown
09	Publication type	0 = News 1 = Background piece 2 = Opinion piece 3 = Audience reaction 97 = Other 99 = Unknown
10a–13a	Actor 1–4	...name...
10b–13b	Role of actor 1–4	0 = Authority figure, United States 1 = Authority figure, European Union/Commission 2 = Authority figure, Netherlands 3 = Edward Snowden 4 = (Representative of) online civil rights organisation 5 = Internet user 6 = Blogger/columnist/journalist, United States 7 = Blogger/columnist/journalist, Netherlands 8 = Scientist 9 = Tech/communication/internet company 10 = Representative of tech company 11 = (Representative of) Dutch Data Protection Authority 12 = Authority figure, Great Britain 13 = Authority figure, Germany 14 = German journalist 15 = Authority figure Sweden

(*Continued*)

(*Continued*)

	Name	Codes
		16 = Whistle-blower (not Snowden) 17 = (Representative of) security agency 97 = Other 98 = Not applicable 99 = Unknown
14	Dominant frame (see Table 2 for an overview of each frame)	0 = End justifies the means 1 = Nothing to hide 2 = Privacy paradox 3 = Empower the user 4 = Privacy is dead 5 = Orwellian dystopia 99 = Unknown