Privacy, Politics and the Fourth Estate

A framing study on the relationship between news media and politics in the Netherlands

---

MA Thesis Seminar: Public Opinion and Political Behavior

Instructor: Dr. M. Meffert

Student: L. Wegewijs

Student number: s1069527

Date: 10 June 2014

Abstract

This thesis compares the use of frames in newspaper articles and parliamentary documents with regard to privacy related events. The objectives are to clarify framing dynamics between Dutch media and parliament, as well as to answer privacy-issue specific questions with regard to framing. Based on two major events demarcating the research period – i.e., the 2001 World Trade Center attacks and Edward Snowden's NSA revelations mid 2013 – it is hypothesized that the way state authorities are framed changes over time from ensuring security towards violating privacy. Furthermore it is hypothesized that changes in privacy frames correspond between similar events and differ between distinct clusters of events. Finally, the 'who-follows-who question' is treated by means of a 'lead/lag' model that compares framing overlap between newspaper articles and parliamentary documents. The data used to achieve both objectives are acquired by coding two Dutch national newspapers (Telegraaf and Volkskrant) and written questions from Dutch parliament for the period between January 1999 and March 2014. Researching this particular period enables to assess the expected dynamics between both arenas between above mentioned landslide events. The data suggest that the expected changes in the way state authorities are frames is absent. The 'lead/lag model suggests that on average media are leading parliament with regard to framing privacy related events. The data furthermore suggests no over-time shift in influence from one arena to the other. Unfortunately, the lead/lag model, as well as the long-term frame dynamics, provides only rough indicators for answering the research questions and assessing the set hypotheses. Therefore, the provided insights are only tentative and ask for further research, so as to deepen understanding about privacy frames and framing dynamics between media and parliament even further.

Table of contents

1. Introduction

On June 5th 2013, British daily newspaper *The Guardian* announced the leak of classified National Security Agency (NSA) documents by whistleblower Edward Snowden[1]. In the months thereafter the widespread nature of NSA's conduct and the level of subsequent privacy violation gradually became clear. Not only ordinary American and foreign citizens were revealed to have been subject to interception and observation; even world leaders like German Chancellor Angela Merkel were found to be monitored[2]. As a result of these revelations, privacy became an important political topic worldwide. In a reaction to Snowden's disclosures, president Obama stated that "[y]ou can't have 100 percent security and also then have 100 percent privacy".[3] Obama's argument to justify NSA's extensive interception and monitoring activities is thus framed as an assumed exchange between privacy and security. The framework of President Obama's argument may be traced back to events roughly twelve years earlier. According to privacy scholar Alan Westin, the privacy landscape had "dramatically changed" in the aftermath of the 2001World Trade Centre attacks (2003, 448). In a response to the attacks, President George W. Bush signed into law the US Patriot Act, an abbreviation for the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (Margulis 2003, 251). This Act provided U.S. authorities with far-reaching possibilities to intercept suspicious information and monitor online activity and individuals (Margulis 2003, 251). In this period, "high public approval of new governmental investigative powers" was measured among the U.S. public (Westin 2003, 448). According to Westin, future attitudes regarding these anti-terrorist measures would likely depend on the occurrence of more successful terrorist attacks and "published accounts of how the government is using its new [post 9/11] powers".

[1] For a timeline, see: http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline
[2] http://www.theguardian.com/world/2013/oct/26/nsa-surveillance-brazil-germany-un-resolution
[3] http://www.reuters.com/article/2013/06/08/us-usa-security-records-idUSBRE9560VA20130608

Mid-2013 Edward Snowden provided for these published accounts by using the media as a means to bring out classified NSA documents. As a result, privacy was put on the worldwide political agenda. The impact of these events also reached Dutch media and politics. Four months after parliamentary debate on the alleged interception of 1.8 million Dutch telephone conversations by NSA, a vote of no-confidence against Minister of Internal Affairs Ronald Plasterk was backed by almost the entire opposition on 11 February 2014[4]. During the years prior to the NSA-affair however, several other privacy-related issues had already been dealt with in both Dutch news[5] media and politics; one example of which is the introduction of the public transport chip card (2009). Proponents of the chip card appealed to the ease of use, while opponents questioned the ability to follow individual travelers. Another example is the long-sought confession in the Marianne Vaatstra case (2012). After thirteen years of investigations a final breakthrough and conviction was made possible by DNA analysis, which stirred the subsequent call for a (mandatory) DNA database. Those in favor of such a database welcome its ability to quickly solve similar crime cases. Opponents on the other hand denounce what they see as treating every citizen as a potential criminal.

A final example is the introduction of nation-wide electronic health records (2008). Whereas proponents see benefits of these electronic health records in reducing unnecessary hospitalizations and minimizing the possibility of medical errors, opponents are afraid of a possible breach of medical confidentiality and hacking medical information. In short, the examples mentioned above not only show the relevance of privacy as such, but also lines out the variety of privacy related events. Privacy is not an event in itself, but an issue that can become salient with regard to a wide variety of events. Besides coverage in national newspapers, written parliamentary questions have been submitted with regard to each of the above events. This overlap between news media and parliament, regarding attention to

[4] http://www.nrc.nl/nieuws/2014/02/12/excuses-en-de-motie-van-wantrouwen-dit-waren-5-belangrijkste-momenten-debat/

[5] Please see Appendix 4 for relevant newspaper articles on these events.

relevant privacy events, would suggest a (reciprocal) relationship between both arenas. This relationship has been researched on both the system-level (Halin and Mancini 2004; Esser et al. 2012) as well as the content-level (Kleinnijenhuis and Rietberg, 1995; Vliegenthart and Roggeband, 2007). The underlying rationale for research into this relationship stems from the assumed mutual influence and interdependency between media and politics and its role in the democratic process.Gadi Wolfsfeld states that while on the one hand, media depend on politicians and government officials for quotes and relevant information, politicians depend on the media in their need of a stage to get their message across (2011, 26). Within the framework of democratic theory, some scholars have even baptized media into the fourth estate (Lewis, Williams and Franklin 2008, 1; Hallin and Mancini 2004, 199), as an additive to Montesquieu's original separation of the legislative, executive and judicial power. According to Alexis de Toquevilles, the press constitutes "the chief democratic instrument of freedom" (as cited in Whitten-Woodring (2009, 595-625). It's this thought that often places independent media at the heart of democratic systems, as a bridge between authorities and the public.

According to Wolfsfeld, the degree of media (in)dependency can be seen as a continuum (2011, 26). The exact point on this continuum is in part determined by the source of information. While media are considered highly dependent whenever authorities possess all or most of all relevant information – as in case of war – the media are highly independent in situations in which media "initiate or uncover critical news stories" (Wolfsfeld 2011, 26). This latter 'media-as-a-watchdog situation' may be exemplified by the NSA disclosures. In this particular case, judging from existing research on the relation between media an politics (for an overview see Walgrave and Van Aelst 2006), it's assumed that the media has had substantial agenda-setting power; i.e., the power to influence *what* is talked about in the political arena. However, it's still unclear to what extent, if at all, media influence the way *how* political actors talk about this or any other particular issue. This how-question is

important because significant framing influence on the political arena by the media would indicate an even larger importance of this institution in democratic dynamics than agenda-setting theory alone would suggest. Therefore, the main research question addressed in this thesis is as follows:

Does Dutch media influence the way in which privacy related issues are framed in the Dutch political arena?

Based on recent developments with regard to Ewards Snowden's NSA revelations, the specific *issue* highlighted in this thesis seems more relevant than ever. Threats to privacy and the respective role of the state as either protector or violator of (the 'right' to) privacy, become more a more relevant. Also due to technological developments and a more and more information driven society. This thesis contributes to the knowledge about the development of the privacy debate in media and parliament in the Netherlands.

This *type* of research, i.e., framing research, is relevant since it provides insight in the extent in which (if at all, not democratically elected) media influence core democratic institutions. On the other hand, it sheds light on the question to what extent, if at all, politics influence free and unattached media. Before moving on however, it's important to point out that the actual research question formulated above strongly suggests a direction of influence; i.e., media is assumed to influence the political arena. However, the reverse may equally well be the case; i.e., the political arena influences media. Partly as a result of the assumed mutual dynamics, the measurement of actual influence may virtually be impossible. The aim is therefore to at least provide insight in broad dynamics between both arenas, which may lead to a result which suggests that one, either or neither of both appears to lead the other with regard to framing privacy related events. In addition, the possible reciprocal nature of dynamics between media and parliament makes it difficult to identify clear independent and

dependent variables. Additionally taking into account the fact that this study is mainly exploratory, this thesis will be structured by research questions and tentative hypothesis, rather than a set of causal hypotheses.

The first of these research questions (RQ1) asks: is media leading politics or is politics leading media with regard to framing privacy related events? A possible indicator of 'influence' could be parliamentary documents refering to newspaper articles. Such a reference would suggests that the parliamentary question is based on a particular newspaper article, which in turn may have influenced the way in which privacy is framed in the parliamentary document. It's expected that parliamentary documents on privacy related events refer to newspaper articles within the article selection of this thesis, which in turn enables to scrutinize similarities and differences in framing privacy between both arenas.

The first hypothesis is based on the assumption that 1) attitudes towards implementation of government safety measures were indeed relatively favorable in the aftermath of the 9/11 attacks (Westin 2003, 448), and 2) due to Edward Snowden's revelations the downside with regard to privacy has become (more) visible. Based upon this it's expected that the role of state authorities has changed over time from protecting citizens against security threats towards violating citizen's privacy. The first hypothesis (H1) states that over the course of the research period state authorities become more visible as privacy violator at the expense of the frame in which state authorities are framed as protecting citizens against security threats. Remaining research questions and hypothesis will be formulated in the following sections.

2. Theory

2.1 Media effect models

According to Van der Eijk, the assumed (reciprocal) relationship between media and politics is considered "hardly more than a truism" (2000, 303). Different ways of measuring this relation have been established. The effect of media content on consumers of media has been researched by means of different models, based on what kind of relation is aimed to be established. Whereas agenda-setting research its main focus is on *which* issues are presented, framing research "helps us to understand *how* salient issues are presented" (Vliegenthart and Roggeband 2003, 296 emphasis added). It can be stated that agenda-setting precedes framing influence, for it is necessary to have an actor to think or talk about a particular issue before it's possible to influence the way in which this issue is formulated. In the wording of Robert Entman, agenda-setting can be regarded as "successfully performing the first function of framing: defining problems worthy of public and government attention" (2007, 164).

However, a possible limitation of agenda-setting theory may be the fact that the media's political agenda-setting power is highly dependent on the course of (world) events, on which media only have so much influence. Media report on events, and logic suggests that news outlets can and will not reasonably ignore important, politically relevant events. Furthermore, it's assumed that politically highly relevant issues will oftentimes reach politicians through official channels anyway; i.e., without the media exercising its intermediary function. It's therefore expected that media possess only limited powers to decide what news is covered and, subsequently, that media's actual political agenda-setting powers might be rather limited.

The aim of this research is therefore to establish the relationship between media and politics, focusing on how privacy related issues are framed. Framing theory, as well as agenda-setting theory, has extensively been researched in relation to public opinion (De

Vreese 2005, 51; Takeshita 2005, 275; Walgrave and Van Aels 2006, 89). However, far less literature exists on the relation between the media and the political arena. Furthermore, Vliegenthart and Roggeband state that the vast majority of research on the relation between media and politics is based on agenda-setting theory (2007, 296). This study attempts to fill the current lack of research on the framing relation between media and politics.

Within literature, framing had been defines in many different ways. Shoemaker and Reese define framing as "modes of presentation that (…) communicators use to present information in a way that resonates with existing underlying schemas among their audiences" (as paraphrased by Scheufele and Tewksbury (2007, 12). According to Robert M. Entman (2003, 417), framing can be defined as "selecting and highlighting some facets of events or issues, and making connections among them so as to promote a particular interpretation, evaluation, and/or solution". Gitlin (1980) describes frames as "principles of selection, emphasis, and presentation composed of little tacit theories about what exists, what happens and what matters" (as quoted in Matthes 2009, 350). Based on these three definitions, it can be stated that framing provides for a tool to take an issue, consciously or unconsciously put it in a conceptual framework, and, without altering the facts as such, influence other's evaluation of the specific issue at hand.

Furthermore, distinctions can be made between different types of frames, three of which will be elaborated here. First, Iyengar (1996) differentiates between *episodic* and *thematic* frames. Whereas episodic frames emphasize specific instances, thematic frames depict issues on a more general or abstract level (Iyengar 1996, 62). In an experimental study, Iyengar examined the influence of these frame types on the evaluation of responsibility for political issues. According to Iyengar, "[t]he two principal types of attributions correspond to causal and treatment responsibility" (Iyengar 1996, 60). Changes between episodic and thematic frames may thus alter the evaluation of perceived causality and assumed treatment responsibility. Although the results show ambiguous degrees of influence among different

issues, Iyengar concludes that the predominance of episodic frames possibly diverts attention from state authorities' responsibilities since episodic frames tend to yield responsibility evaluations on an individual level (1996, 70).

Second, De Vreese and Semetko (2001) differentiate between issue-specific frames and generic frames (see also Matthes 2009). Whereas issue-specific frames "pertain to the particular issue in question" (De Vreese 2005, 55), generic frames "can be identified across different issues" (Matthes 2009, 350). Based on existing research, Semetko and Valkenburg (2000, 95-6), differentiate between five "commonly occurring" or generic news frames: conflict, human interest, economic consequences, morality and responsibility. In their study, Semetko and Valkenburg aim to compare the use of these frames across different types of issues as well as across different types of media outlets. According to Vliegenthart and Roggeband (2007, 300), "[parliamentary] documents differ in significant respects from newspaper articles". The authors maintain that this difference complicates identifying generic frames in parliamentery documents. Therefore, since this thesis comparares media and parliament, this type of frames is not used here.

Third and final, Chong and Druckman (2007) point out the distinction between *equivalency* and *emphasis* frames. In short, equivalency frames are "different, but logically equivalent (…) phrases", put to use as to "cause individuals to alter their preferences" (Tversky & Kahneman, as quoted in Chong and Druckman 2007, 114). Emphasis frames, on the other hand, "focus on qualitatively different yet potentially relevant considerations" (Chong and Druckman 2007, 114). Emphasis framing enables to identify particular aspects with regard to privacy related events. Putting emphasis on different aspects results in a different frame. This approach is similar to what Matthes and Kohring describe as "patterns frames", which are "[f]rames as clusters of frame element" (2008, 263). In this approach, corresponding emphasis on, or corresponding combinations of particular frame aspects between media and parliament would suggest that media and parliament frame privacy related

events in the same way. Due to the versatile nature of privacy, as elaborated in the coming pages, an approach similar to this latter method of identifying frames is used this thesis.

2.2 Privacy

The reason why privacy is a subject that deserves to be researched in relation to politics is that it plays a significant role in the relation between the state and its citizens. According to Alan Westin (2003, 433), "[e]very society sets a distinctive balance between the private sphere and the public order". Society may disapprove of certain behavior, and therefore maintain that privacy claims with regard to this particular behavior are invalid (Westin 2003, 433). Privacy has therefore often been viewed as an "effective way to keep government out of the lives of private individuals and institutions" (Nissenbaum 1998, 568). However, the conceptual scope of privacy, as well as the question of exactly what behavior is covered by privacy and what is not, remains "debatable" (Margulis 2003, 244) and is "hard to define precisely" (Van Lieshout et. al. 2013, 120). For a complete overview of conceptualizations, see Smith, Dinev and Xu (2011, 992).

Westin (2003, 431) defines privacy "as the claim of an individual to determine what information about himself or herself should be known to others". This conceptualization suggests the presence of privacy violation whenever agencies or authorities other than the relevant actor itself lay claim to this judgment, regardless of the relevant actor's (tacit) consent. This self-determination seems to be a constant factor in privacy conceptualizations. According to Margulis for example, "[p]rivacy, as a whole or as a part, represents *control* over transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability"(1977, 10 emphasis added). This notion of privacy-as-control is however criticized by Graeme Laurie, who states that it is both unrealistic and unfeasible. According to Laurie, this definition would essentially render any

day-to-day, basic human interaction a compromise to privacy (as paraphrased in Taylor 2012, 17).

This basic and very incomplete outline of what privacy actually means, seems to show an element of truth in BeVier's statement that "[p]rivacy is a chameleon-like word, used denotatively to designate a wide range of widely disparate interests" (1995, 458). Although this thesis will not discuss the normative debate on privacy (violation) and its consequences, basic understanding of the concept of privacy may provide a better understanding of how this issue *can* be framed. According to Stephen Margulis, privacy issues can be divided into four distinct branches: "citizen-government privacy, consumer privacy, medical and genetic privacy, and workplace privacy" (2003, 250). As shown in figure 1, these branches are subjects, each expected to conjoin a variety of more specific privacy-related events.

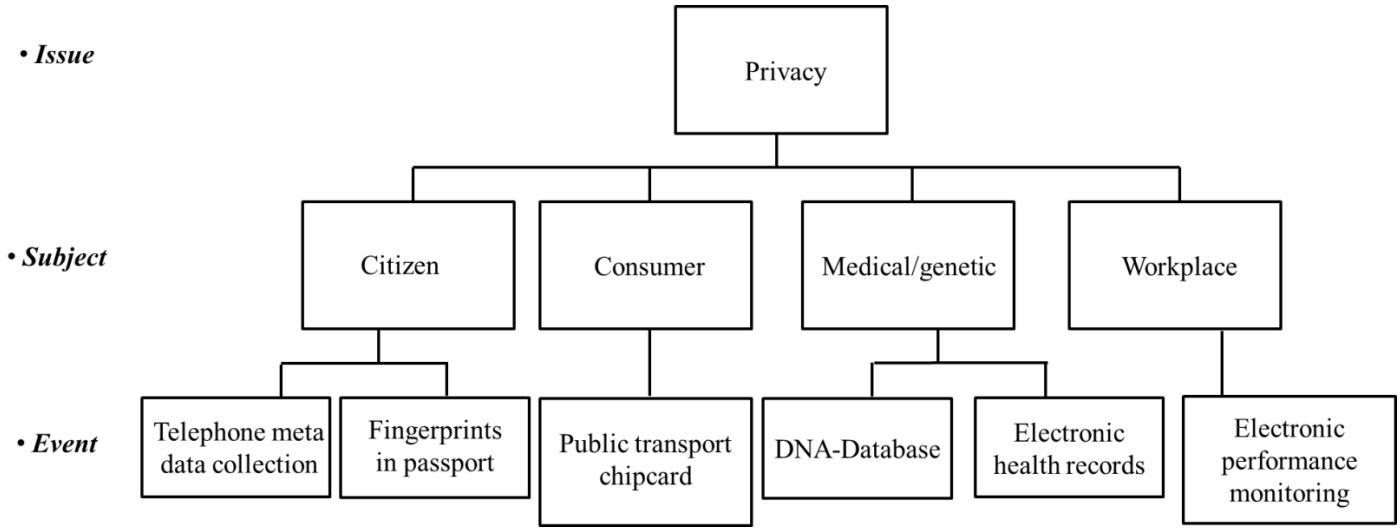

Figure 1: Hierarchy of privacy issue, subjects and events (based on Margulis 2003).

In addition, Margulis identifies three positions in privacy debates: the high-privacy position, the balanced-privacy position, and the limited-privacy position (2003, 250). These privacy positions correspond to the degree of importance assigned to privacy and its relation to other interests. Margulis' privacy positions seem to correspond with findings by Marc van Lieshout et. al., who state that the relation between privacy and security is traditionally

modeled in a trade-off structure (2013, 119). This trade-off structure suggests a negative correlation between both concepts. While an increase in the level of security is suggested to cause a decline in the level of privacy, an increasing level of privacy is suggested to limit the level of security. Although Van Lieshout et. al. demonstrate that this reasoning is flawed, for privacy and security are argued to be heavily intertwined and inseparable concepts, it's expected that the privacy debate within the defined research period has at least partly been based on these perceived trade-off dynamics.

A relevant question, based on Margulis' distinction between different subjects of related privacy events, is whether change in the use of particular frames in one subject results in a similar change in other subjects. In other words: does a peak in the visibility of a particular frame regarding the citizen privacy subject, lead to similar dynamics with regard to the medical/genetic or consumer privacy subject? It's expected that privacy is an umbrella issue that covers a multitude of events that cluster together in independent subjects. An answer to this question sheds light on the level of homogeneity of the privacy issue. If frame changes regarding events within subjects occur independent of frames with regard to another subject, this would suggest that subject – or clusters of events – are likely to have their own independent dynamics; which in turn confirms the expected variety of this subject. Unfortunately, framing literature provides no information on this. Therefore, a tentative hypotheses is formulated; tentative in the sense that the hypothesis' direction is logic-based rather literature-based. The second hypothesis (H2) states that an increase in the use of a particular frame in one privacy subject only influences the use of frames within this particular subject.

3. Methods

In order to identify emphasis on particular frame component aspects, so as to identify different frames, content analysis is used. According to Harold Lasswell, content analysis' main purpose can be defined as to identify "[w]ho says what, to whom, why, to what extent and with what effect?" (1948, 28). Earl Babbie conceptualizes content analysis as "the study of recorded human communication, such as books, websites, paintings and laws" (2003, 333). Broadly, regardless of the specific frame definition and approach of measuring these, two types of methods to identifying frames can be distinguished: inductive and deductive. Whereas deductive methods make use of predefined frames, inductive methods refrain "from analyzing news stories with a priori defined news frames" (De Vreese 2005, 53). According to De Vreese, most scholars have advocated in favor of the deductive method (2005, 53). Whereas Vliegenthart and Roggeband make use of predefined frames obtained in a "qualitative pre-study" (2007, 300), this method may in this case not be appropriate. Based on Westin's work, it's assumed that the 2001 World Trade Center attacks have shaken the "privacy landscape" (2003, 448). Therefore, a priori identifying frame aspects in a small article selection outside the research period may result in aspects that cannot adequately cover the research period content. In other words, a preliminary study based on a small article and document selection outside the research period may result in frame aspects that are likely to – at least to some extent – misrepresent the frames that occur in the actual article selection. The specific aspects of frame components such as problem and solution definition, perceived victims, perpetrators and privacy definition, largely based on Vliegenthart an Roggeband's "list of sensitizing question to code frames" (2007, 335), will therefore be obtained from the actual article selection. This back-and-forth, switching between inductive and deductive methods while coding and recoding, will yield relevant frame aspects related to privacy events within the newspaper article and parliamentary document selection.

In this research the units of analysis are newspaper articles and written parliamentary questions. The variables that are used are privacy frames in media and privacy frames in the political arena. As discussed above, clear independent and dependent variables are not directly identifiable since the direction of 'influence' may go both ways. The first research question therefore asks which of both arenas appears to be leading in framing privacy related events.

The degree of framing 'influence', however, is likely to be subject to choices in research design – i.e., framing effects could be higher or lower as a result of design choices, independent of actual framing influence. Walgrave and Van Aelst (2006, 94) elaborate multiple *agenda-setting* research design choices and their respective implications. Partly due to the fact that Vliegenthart and Roggeband assume these implications to be similar in framing research (2007, 298), one of these research design choices will be taken into account in this thesis.

According to Walgrave and van Aelst, one comprehensive political agenda cannot be identified (2006, 94-5). In fact, many political actors have one or more individual agendas. A distinction is made between substantial and symbolic political agendas (Vliegenthart and Roggeband 2007, 297). Whereas the latter represents a more flexible agenda of rhetoric, the former has to do with actual policy and legislation (Walgrave and van Aelst 2006, 94). Existing research seems to show higher agenda-setting influence on the political arena in cases of symbolically defined political agendas (Walgrave and van Aelst 2006, 95). As mentioned earlier, agenda-setting is oftentimes regarded as to precede framing. Therefore, a symbolic defined agenda is assumed to yield relatively high media framing influence.

3.1 Content categories and coding scheme

The research method used in this study corresponds to the methods proposed by Matthes and Kohring (2008). In this way of measuring frames, as Matthes and Kohring put it, "frames are neither identified beforehand nor directly coded with a single variable" (2008, 264). This method is based on Entman's earlier mentioned definition of a frame. According to Matthes and Kohring (2008, 264), in this definition a frame consists of several components. These components, based on Entman's definition are: problem definition, causal interpretation, moral evaluation and treatment recommendation. Together these distinct components form a frame. This thesis makes use an extended list of components, based on Vliegenthart and Roggeband's "list of sensitizing question to code frames" (2007, 335). The reason for this extension is that this thesis is interested in the role of particular actors with regard to privacy related eventen.

In this thesis the following six frame components are taken into account: problem definition, perceived cause, perceived perpetrator, perceived victim, solution definition and solution executor. In addition, the privacy definition used in articles or documents is recorded. As visualized in Figure 2, for each of these seven frame components one out of multiple aspects can be identified and coded. These aspects are partly based on existing literature, and partly inductively obtained from the newspaper articles and parliamentary documents The coding scheme, or complete list of frame components and their respective component aspects, can be found in Appendix 1. In some cases, multiple frames are identified. For these articles and documents, more than one 'combination of frame component aspects' is recorded.

The first component relates to the *privacy definition* used in newspaper articles and parliamentary documents. Maybe the most obvious definition, based on privacy literature, is 'privacy vs. security' (Westin 2003, 438; Margulis 2003, 247; Epstein, Roth and Baumer 2014, 160). Since privacy is set against non-security interests as well, multiple 'privacy vs.

[interest]' definitions have been identified and inductively added to the coding scheme. Other privacy definitions based on literature (Smith, Dinev and Xu (2011, 992) are 'privacy as a state', 'privacy as control', 'privacy as a commodity' and 'privacy as a (human) right'. An example of an article in which two 'combinations of frame component aspects' have been coded can be found in appendix 4 (*"Dubbel slot op medisch dossier"*, Telegraaf, 31 january 2011). In this article on 'electronic health records' both 'privacy as control' and 'privacy vs. [interest]' have been coded.

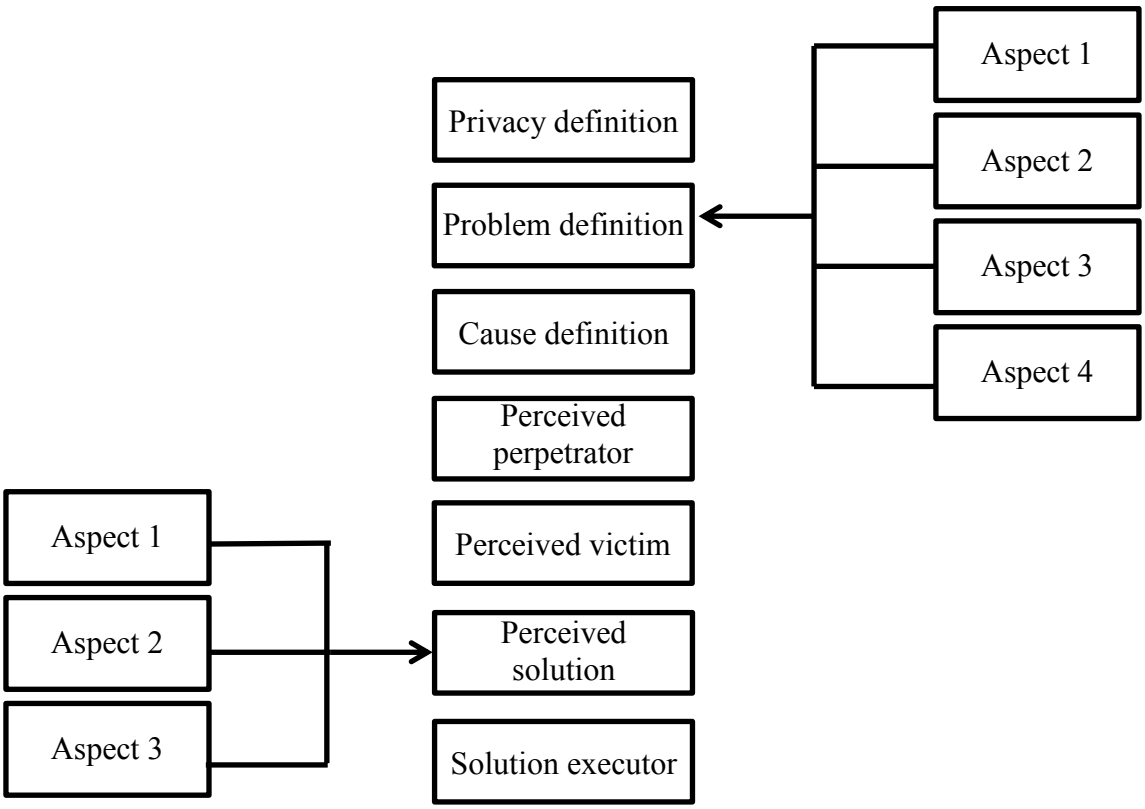

Figure 2: Frame components and frame component aspects

For the second component, five *problem definitions* are used to code the central problem in each article and document. Besides 'privacy violation', two 'external' problem definitions are identified: security related and non-security related. Whereas 'external threat(s) (security)' obviously relates to situations in which threats to security are deemed to be central problem, 'external threat(s) (non-security)' relates to cases such as information unavailability.

The fourth aspect ‘economic consequences’, is recorded with regard to ineffective marketing and buisinessmodels based on trading information. Economic consequences are also recorded in cases in which a deliberate choice is made to ‘pay’ with privacy. An example of this interpretation can be found in Appendix 4 (*“Webzoeker GX staat vlak voor doorbraak in VS”*, Telegraaf, 8 September 2012). Frame component aspect ‘other’ is recorded for problem definitions other than the four elaborated above.

The third component is closely related to the second. *Cause definition* tells what is perceived as the cause for the problem definition. A distinction is made between five aspects. The first two aspects, ‘(too) far reaching of interception’ and ‘(undesired) disclosure of information’, are related in the sense that they both represent situations in which privacy may be under pressure. They are distinct because the former indicates a deliberate and targeted interception while the latter is identified in cases in which (personal) information (may) come out; due to poor safety measurements for example. An example of ‘(too) far reaching of interception’ can be found in Appendix 4 (*“Privacy verdient ook na 11 september bescherming”*, Volkskrant, 2 October 2001). In this article both privacy definion ‘privacy as a (human) right’ and ‘privacy vs. security’ are aslo visible. In contrast to the first two, ‘the third aspect holds that the perceived problem is caused due to ‘(too) far reaching of privacy protection’. The fourth and fifth aspects are ‘security threat(s)’ and ‘non- security threat(s)’.

The fourth and fifth component, i.e., *perceived perpetrator* and *perceived victim*, provide insight in who is deemed responsible for and who’s subject to the perceived problem. The *perceived perpetrator* component is coded as either ‘state authorities’, ‘corporate enterprices/media/health industry’ or ‘terrorists/criminals/lawbreakers/individual actors’. In practice the component aspects are rather broad categories. For example political party leaders, supranational political institutions and government officials are all coded as ‘state authorities’. For frame component *perceived victim* straightforward aspects are coded. Frame component aspects ‘citizens’, ‘employees’, ‘patients’ and ‘consumers’ correspond to

Margulis' privacy subjects. In addition, 'society/corporate (media) interests' has been coded whenever a more broad – yet non-governmental – perceived victim is identified.

The sixth and seventh component shed light on the *perceived solution* and who's deemed to solve the problem respectively; i.e., the *solution executor*. Broadly, *perceived solution* consists out of two branches which in turn consist of two aspects. Components aspects 'expand privacy protection' and 'don't publish/provide (personal) information' are coded whenever privacy violation is perceived to be prevented or resolved. The difference between both aspects has to do with the nature of resolve. Whereas 'expand privacy protection' is coded for institutionalized prevention like rules and regulations, 'don't publish/provide (personal) information' is coded whenever the solution is perceived to be in (individual) decisionmaking with regard partaking in information distribution. Examples can be found in Appendix 4(*"Fiscus mag niet altijd snuffelen"*, Telegraaf, 27 November 2013 and *"Ik dacht direct: 'weg ermee!'"*, Volkskrant, 21 February 2014). This latter article is also an example of *privacy definition* 'privacy as a commodity'.

3.2 Full-frames and partial-frames

During the coding process frame components elaborated above will be treated as independent categories. In the analytical phase of the study 'combinations' of frame component aspects will be assessed based on a priori expectations; i.e., the visibility of certain expected combinations of frame component aspects may show up more often than others. The visibility of particular aspects over others provides insight on which aspects emphasis is put, and subsequently how privacy related events are framed in both areas under consideration.

As outlined above, for each newspaper article and parliamentary document seven distinct frame components are coded. The main question here is: how many aspects make a frame? With seven components coded for each item, the obvious way to go about would seem

to investigate the count of unique frame aspect combinations, consisting of all seven components, and correlate the count of these unique combinations of frame component aspects between media and parliament over time. As visualized in Figure 3, taking into account all seven components yields what is here referred to as a 'full-frame'. Full-frames are distinct from partial-frames, which do not include all seven, but at least two components. A strong correlation between media and parliament with regard to the visibility of a particular aspect combination which contain all seven components – i.e., with regard to a full-frame – is assumed to be a more relevant finding than a similar correlation coefficient between media and parliament with regard to a combination which contain fewer components – i.e., with regard to a partial-frame. The rationale behind this lies in the fact that a combination of only two or three frame components may result in counting frames from articles that would be strictly separated if a particular additional component enters the equation.

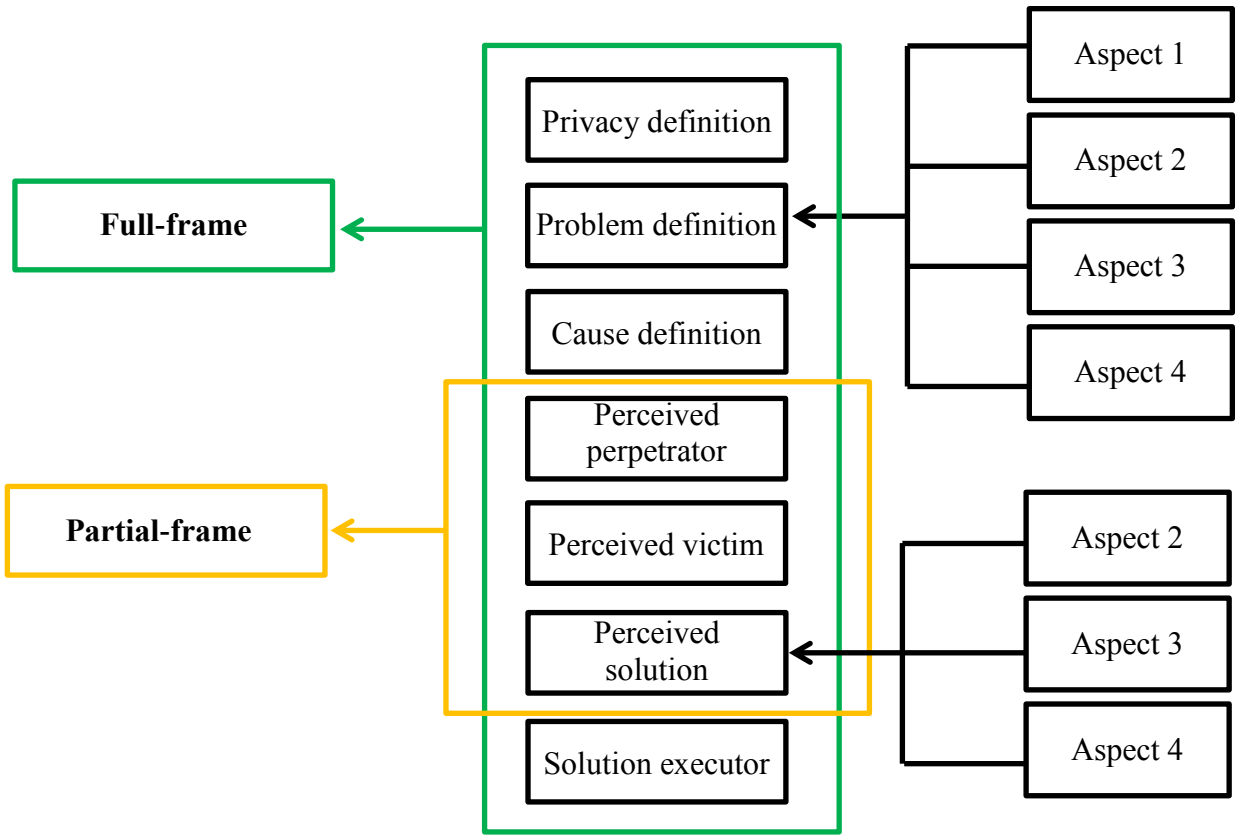

Figure 3: Full-frames, partial-frames, frame components and aspects.

Nonetheless, a distinction will be made between full-frames and partial frames. This distinction is justified by the assumption that sticking to a seven-indicators-make-a-frame-prerequisite results into low numbers of unique frames; too low to reasonably compare both arenas based on quantitative data. This is especially so since it's expected that these frames are visible with regard to multiple distinct privacy related events, which reduces the amount of comparable frames even further. It's logically expected that unique partial-frames yield higher counts than unique full-frames. This trade-off between quality and quantity may ideally be undesirable, but practically necessary so as to be able to compare long-term frame dynamics between both arenas.

3.3 Newspaper article and parliamentary document sample

The media arena is represented by two national newspapers: Volkskrant and Telegraaf. These newspapers roughly represent left and right political views respectively (Sematko and Valkenburg 2000, 97). Obviously, this representation of media does injustice to the much wider range of different news sources, like television, radio and social media that potentially influence the political arena. The relative *agenda setting* impact of each of these sorts of media is subject of debate. A debate that is, according to Walgrave and Van Aelst, "far from settled" (2006, 92). This disputed level influence on the political arena, with regard to different types of media, is likely to be similar with regard to framing influence. However, the decision to analyze newspaper media only can be justified based on findings by Weber Shandwick, a The Hague based research office. Their recent research shows that the majority of Dutch MPs see traditional newspapers – both print and digital versions – as the main news medium (Weber Shandwick 2014).

The newspaper articles analyzed in this study are collected by running the following search string through LexisNexis Academic, for the period between 1 January 1999 and 1 April 2014:

> HLEAD (Privacy! AND Veiligheid! OR Recht OR NSA! OR DNA! OR Dossier! OR Telefoon! OR OV Kaart OR OV-Kaart OR OV OR Consument! OR Burger! OR Informatie! OR Patiënt! OR Werknemer!)

The section search HLEAD narrows down the amount of articles to a set of articles in which privacy is mentioned while connected with at least one of the other terms in either or both an article's title or lead. Without title-lead limitations the number of articles would be far beyond the feasibility of this thesis. This is partly due to the fact that this research covers almost 15 years. The choice of this period is based on the fact that it encompasses a time period not only delimited by two major international events in the international privacy debate – i.e., 9/11 and the NSA affair – but also subject to rapid developments in the field of communication and information availability. Some commentators have labeled the relation between these latter developments and (individual) privacy as both evident and irreversible (Westin 2003, 441-2).

The search terms represent the relation between privacy on the one hand, and on the other hand security, perceived right to privacy and or security, the NSA affair, DNA related events, health record related events, mobile communication, public transport chip card related events, consumers, information in general, patients and employees. The exclamation marks ensure that articles with words with extensions to these search terms are included in the selection as well. This search string is has yield a relevant, representative and yet still manageable overview of privacy coverage in Dutch media. It's likely that substantial numbers of newspaper articles – as well as parliamentary documents – deal with privacy related

subjects and events, without mentioning the actual word 'privacy'. Based on the applied search string, these articles will not be included in the article sample. Although this is a shortcoming in the selection procedure, including these articles would however not be feasible within the boundaries of this thesis. Based on the aearch methods outlined above, a total of 662 newspaper articles from Volkskrant (410 articles) and Telegraaf (252 articles) have been selected.

The political arena is defined as the Second Chamber of the Dutch States General, and operationalized as written parliamentary questions and answers to these questions. As argued above, parliamentary questions might be regarded as merely symbolic, and therefore fail to provide for a representative picture of media impact on the political arena. However, since the framing relation between media and politics has not been researched that often, making use of a symbolic agenda provides for a critical case. If media's framing power is found to be low, it cannot reasonably be expected that media's framing power will be more substantial with regard to substantial agenda's such as party manifestos, coalition agreements or legislative proposals. The parliamentary documents are obtained from www.officielebekenmakingen.nl. A search on ‘privacy’ within the category ‘Kamervragen met antwoord (Aanhangsels)’ in the period between 1 January 1999 and 1 April 2014 results in a total 715 parliamentary documents

3.4 Relevant newspaper articles and parliamentary documents

The total number of newspaper articles and parliamentary document within the article and document selection has been reduced as a result of irrelevant articles which have been excluded from the final analysis. In total, 187 newspaper articles and 302 parliamentary documents have been excluded, resulting in 475 relevant newspaper articles and 413 relevant parliamentary documents. Newspaper articles in which privacy is only mentioned in passing or referred to in an enumeration are not taken into the final analysis. Parliamentary documents

are excluded whenever privacy is only mentioned in passing, referred to in an enumeration or mentioned in a sentence that reads something similar to "for privacy reasons I can unfortunately not go into that". This latter kind of exclusion applied for a large part to documents from 2006/2007, since at that time the Dutch integration and asylum debate took off.

The over-time distribution of relevant newspaper articles and parliamentary documents is shown in figure 4. As expected, an upward trend for the number of newspaper articles and parliamentary documents on privacy related events is visible. This resembles the increasing attention to privacy as such in recent years. The sudden increase of newspaper articles between 2008 and 2010 and in 2013 is due to coverage on subjects as 'medical confidentiality' (2008), privacy of convicts (2009) and privacy of suspects (2010). Privacy event '(electronic) health Records' is visible though each of these years, including 2013, in which privacy event 'NSA/PRISM' boosts the number of newspaper articles. The long-term trend correlation coefficient between media and parliament is high (r=.71), which indicates that in both media and parliament the amount of privacy related articles are increasing over the research period.

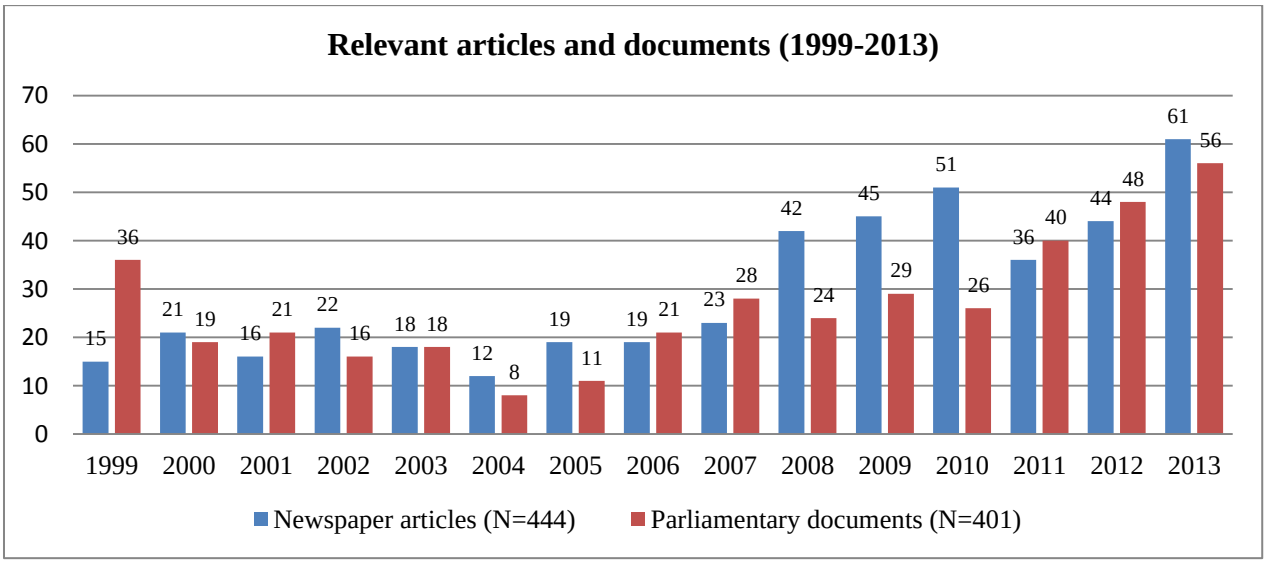

Figure 4: Relevant newspaper articles and parliamentary documents (1999-2013). Long-trend (r=.71), short-term fluctuations correlation (r=-.20).

Note that in this and following Figures, as well as in most the analytical part of this thesis, data from 2014 is ignored. This is done since this for this year only three months have been coded. Including this year would either falsely suggest a drop in the amount of articles, documents and frames, or necessitate undesirable extrapolation of the 2014 data.In some of the newspaper articles and parliamentary documents, multiple frames or sets of frame component aspects are identified. In these cases, multiple sets of aspects have been recorded. The distribution of these frames is visualized in figure 5. In the period 1999-2014, 450 sets of frame component aspects are identified in parliamentary document and 627 sets of frame component aspects are identified in newspaper articles; a total of 1077 sets of frame component aspects. Like the newspaper articles and parliamentary documents in which these frame component aspects are identified, the long-term trend correlation between media and parliament is high (r=.77).

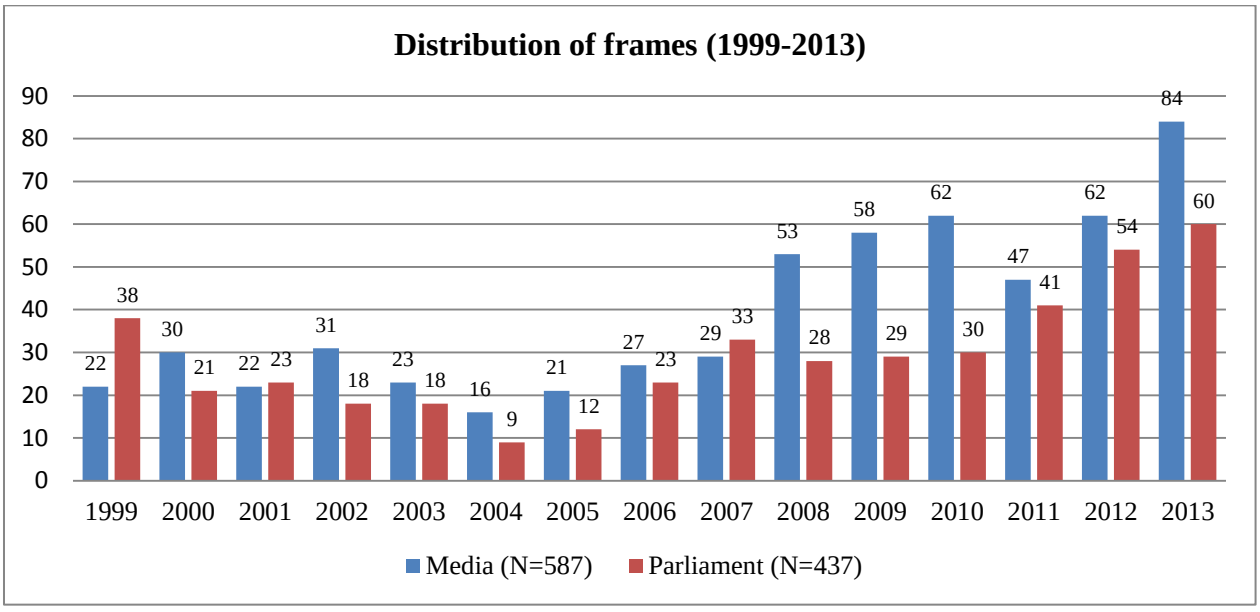

Figure 5: Distribution of frames (1999-2013). Long-term trend correlation (r=.77), short-term fluctuations correlation (r=-.06).

4 Results

4.1 Parliamentary document references

Within the parliamentary documents, oftentimes references to other documents are made. Overall, 101 unique sources have been identified and recoded into one of eight groups: national newspapers, print press (other), free newspapers, internet, news sites, other, parliamentary documents and RTV. Some of these sources have been referred to more than once. Figure 6 shows that 118 out of 298 references, or 39.6% of all references, refer to Dutch national newspapers (De Telegraaf, Volkskrant, NRC, Algemeen Dagblad, Trouw, Parool and Financieele Dagblad). This corresponds to earlier mentioned findings by Weber Shandwick (2014), who found that the majority of Dutch MPs see traditional newspapers – both print and digital versions – as the main news medium.

Of these 118 newspaper references, 37 refer to Telegraaf and 27 to Volkskrant content. Since parliamentary document almost always refer to source and date only, it's not possible to identify the exact articles referred to in these documents. Only 16 newspaper article titles are explicitly mentioned, 5 of which originate from Volkskrant and 11 from De Telegraaf. Neither of these articles however, are part of the Lexis Nexis newspaper selection obtained for this study. This implicates that, based on the search string that has been used, MP's ask or answer questions in which the word privacy is mentioned, referring to articles in which the word privacy is not mentioned.

The fact that the assessed parliamentary documents do not refer to articles within the article selection invalidates the basis for establishing any direct connection between media frames and parliamentary frames in this study; i.e., this deprives the opportunity to state that based on this particular newspaper article using that particular frame, this parliamentary question, using the same or a distinct frame, has been issued. Therefore, only a rough indication can be provided on the framing connection between both arenas.

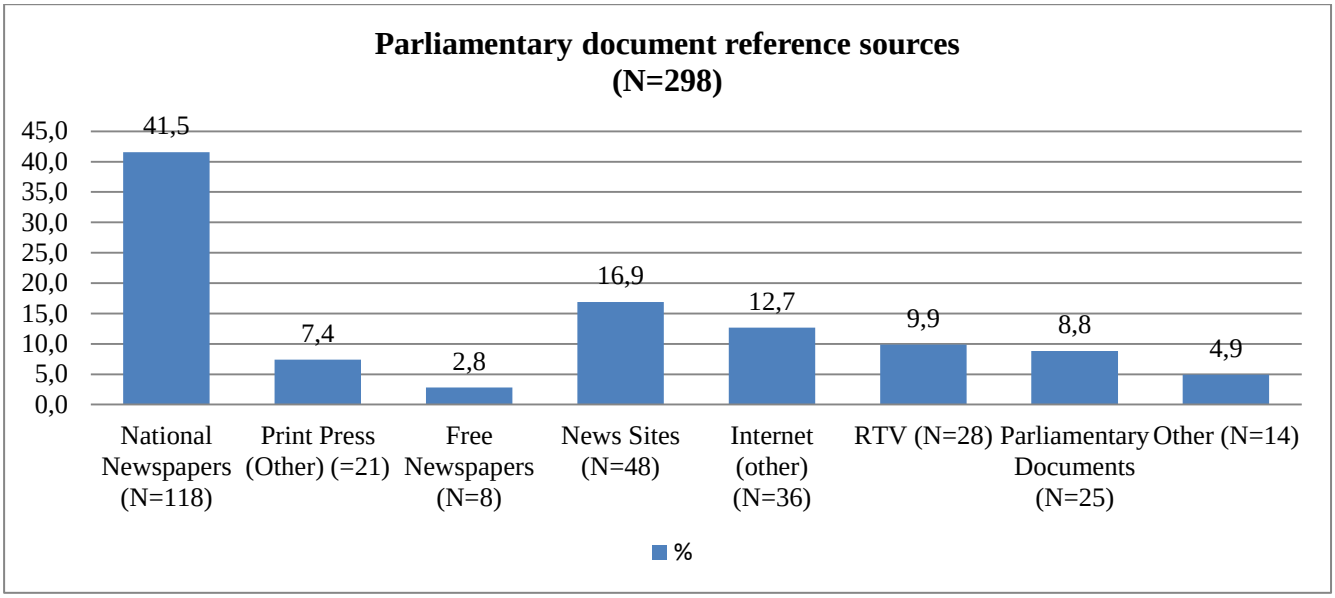

Figure 6: Parliamentary document references (1999-2014).

4.2 Individual and clustered frame component aspects

As discussed in the methods section, privacy frames are identified by coding newspaper articles and parliamentary documents based on seven frame components. As visualized in Table 2, for each of these components, multiple 'response options' or indictor aspects have been used to code the content of newspaper articles and parliamentary documents. In Table 1, an overview is provided of each individual component aspect and the count of these in newspaper articles and parliamentary documents. In addition, correlation coefficients for both long-term trends and short-term fluctuations are included. Long-term correlation coefficients between media and parliament are calculated by simply correlating component aspect counts in each arena over the length of the research period. Short-term fluctuation correlations, on the pother hand, are calculated by subtracting previous year's component aspect count from the component aspect count of each individual year, and correlating these per year change figures between media and parliament over the length of the research period. In the latter case, the first year of the research period (1999) will not be included, for there is no component

aspect count for its preceding year (1998) that can be subtracted so as to calculate 1999's change figure.

Frame component aspects	Count		Media-parliament correlation coeficient	
	Media	*Parliament*	*Long-term trend* (r=)	*Short-term fluctuations* (r=)
1. Privacy definition				
Privacy as a (human) right	83	37	.23	.07
Privacy as a state	45	44	.26	-.15
Privacy as control	161	93	.69	-.30
Privacy vs. Other interest(s)*	187	151	.35	.17
2. Problem definition				
Economic consequences	46	24	.79	.53
External threat(s) (non-security)	70	40	.14	.24
External threat(s) (security)	84	41	.23	.24
Privacy violation	375	328	.76	-.17
3. Cause definition				
Interception/(undesired) disclosure*	346	286	.75	-.15
(Too) far reaching of privacy protection	73	32	.04	.30
Non-security threat(s)	92	71	.85	.66
Security threat(s)	66	33	.35	.32
4. Perceived pepetrator				
Corporate enterprises/media/health industry	156	123	.64	-.19
Other	71	68	.16	-.55
State authorities	153	110	.61	.18
Terrorists/criminals/lawbreakers/individuals	142	61	.66	.47
5. Perceived victim				
Citizen(s)	314	221	.54	.19
Consumer(s)	84	66	.91	.68
Employee(s)	33	19	.37	.07
Patient(s)	61	60	.74	.65
Society/corporate (media) interests	56	22	.23	-.24
6. Perceived solution				
(Expand) Privacy protection*	217	149	.59	-.31
Decrease privacy protection*	138	55	.60	.61
7. Solution executor				
Corporate enterprices/Media	91	34	.74	.42
Judiciary	42	18	.15	.00
Other	56	31	.25	.20
Societal groups/individuals	56	11	.34	.16
State authorities	184	277	.61	-.33

*Table 1:Long-term and short-term correlation coefficient for individual frame component aspects. *Recoded into one variable, as clearifiedin Appendix 1.*

Table 1 suggest that for most individual component aspects there are medium to high levels of merely positive correlation between both arenas. This is an indication of an overall upward trend that can be explained by the increasing attention for privacy related issues in general, in both media and parliament. However, these long-term trend correlations provide no insight in whether short term fluctuations in these overall developments occur at the same time. Short-term fluctuation correlation coefficients per component aspect enable to investigate whether changes in the visibility of particular component aspects occurs at the same time. In this case at the same time implies visibility in the same year. These short-term fluctuation correlation levels are but a few exceptions lower, and sometimes even negatively correlated. Out of 28 component aspects taken into account, only 13 component aspects show short-term fluctuation correlation figures of (r=0.30) or higher, or (r=-.30) and below, with the highest correlation for perceived victim 'consumer(s)' (r=.68). This suggests that with regard to individual frame component aspects, there is no apparent relationship between both arenas. However, one frame aspect component does not really tell a story. Even if there would be high correlation coefficients between media and parliament for the majority of individual component aspects, only combinations of these component aspects shed light on how the Dutch privacy debate has really developed over time. In fact, due to combinations with other component aspects, a single aspect could be part of virtually opposing frames. The effective meaning of component aspects comes with combining individual component aspects into actual frames.

Automaticaly retreiving the count of unique combinations including all seven frame components, results in a total of 688 unique full-frames. In this count all coding options, including 'N.A.' and 'other', have been taken into account. In addition, some component aspects that have been coded separately have been recoded into one component aspect so as to yield higher counts per full-frame (see Appendix 1). Out of these 688 unique component aspect combinations only 11 full-frames appeared at least ten times. The most frequently

occurring frame appeared 25 times across media and parliament combined, representing roughly 23 % of all visible frames. The long-term trend correlation coefficient of this most frequently occurring full-frame is medium (r=.27). The short-term fluctuation correlation coefficient is also medium (r=.37). Although this full frame becomes more visible over time in both arenas and shows a medium level short-term fluctuation correlation, the actual frame counts are relatively low. Furthermore, this full-frame is dispersed over 17 different privacy events, visible either in media or in parliament. This suggests that it's not realistic to require a combination of all seven frame components before taking a frame into account. Doing so would lead to the inability to compare media and parliament.

The number of mathematically possible partial-frames, i.e., frames with a number of incorporated components fluctuating from 2 to 6, however, is virtually infinite. Based on privacy literature reviewed above, certain frame aspects are expected to cluster together, i.e., converge into a (partial-) frame. Furthermore, starting off with one expected component and adding additional expected components one by one, sheds light on exactly which component(s) are key in certain frames and their dynamics in media and parliament respectively. In the following section each additional component will be elaborated so as to clarify the potential influence of these additional components on frame dynamics.

4.3 Privacy vs. other (security) interest(s)

As elaborated above, in privacy literature, privacy is oftentimes mentioned as an interest opposed to other interests. In the aftermath of the 9/11 World Trade Center attacks in 2001 many safety measures have been adopted. The role of the state in this respect is expected to have changed from being framed as a protector of citizens against security threats in roughly the first half of the research period, towards privacy violator in the latter half of the research period. The first hypothesis (H1) states that over the course of the research period the frame in which government is portrayed as privacy violator becomes more visible at the expense of the

frame in which government is portrayed as protecting against security threats. Based on the trade-off nature of these frames, it's expected that both frames are based on *privacy definition* 'privacy vs. other interests'.

In order to assess this hypothesis, a priori expected combinations of particular frame aspects will be investigated. Starting off with privacy definition ‘privacy vs. other interests’ provides a commonly used definition according to both privacy literature (Reference) and this research’s data (visible in roughly 34% of all recorded frames). For this individual component aspect, the long-term trend correlation is moderate (r=0.35). Short-term fluctuations show a low negative correlation between media and parliament (r=-.17). Based on the nature of this privacy definition two additional component aspects seem to make sense.

First, *problem definition* 'privacy violation’ and ‘external threat(s) (security)’ have been added respectively. These two partial-frames show different correlation dynamics between media and parliament. The privacy violation frame shows a low correlation coefficient (r=.13) between media (N=73) and parliament (N=71) regarding long-term trend. The short-term trend correlation coefficient is substantial (r=-.41). With regard to the security threats frame, media (N=56) and parliament (N=36) show a low correlation coefficient (r=.25) for the long-term trend and, again, a substantial level of correlation (r=.39) for short-term fluctuations.

Focusing only on the second half of the research period (2006-2013), this contrast between the privacy violation frame (r=-.69) and the security threats frame (r=.53) is even larger. Checking the correlation coefficient for this latter half of the research period stems from the above mentioned increase of relevant newspaper articles and parliamentary documents from 2006 onwards. The increase in articles and documents as well as the amplification of correlation figures suggest that the issue of privacy and it’s assessment has changed midway the asseded research period.

The counts for the security threat frame are relatively low in both arenas, especially parliament. Combining problem definitions ‘external threat(s) (security)’ and ‘external threat(s) (non-security)’ – so as to virtually create two partial-frames representing both sides of a trade-off between privacy and both security and non-security problem definitions – results in higher counts in media (N=91) and parliament (N=68). Furthermore, this frame shows higher correlation levels than the partial frame in which only ‘extern threat(s) security’ is taken into account. This is visible for both long-term trends (r=.32) and short-term fluctuations (r=.49). Again, the correlation coefficient for short-term fluctuations in the second half of the research period (2006-2013) is higher (r=.67).

The dynamics described above seem to suggest that both frames increase on the long run. In the short-term media and parliament agree on identifying security threat(s) as problem definition in conjunction to a *privacy definition* which identifies a trade-off between privacy and other (security) interests. With regard to identifying privacy violation as problem definition in a trade-off environment on the other hand, media and parliament show contrary short-term dynamics. It should be noted that ‘short-term’ is only a relative concept, which in this particular case means year-to-year. This leaves plenty of space for absence of connection between both arenas, but nevertheless provides a usefull insight in over-time dynamics.

The findings elaborated above are supported by correlation figures between media and parliament dynamics with regard to *opposing* problem definitions, i.e., the correlation between media’s problem definition ‘privacy violation’ and parliament’s problem definition ‘external threat(s)’ and *vice versa*.

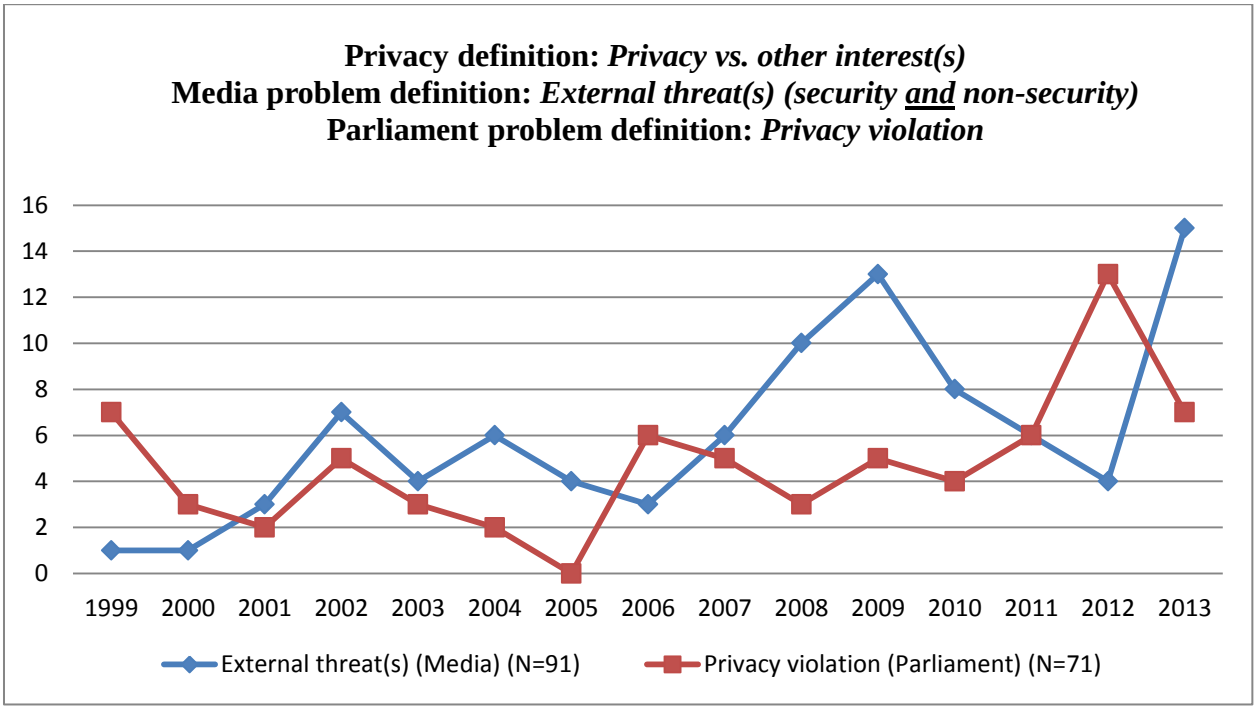

Figure 7: Comparing opposing frames between media and parliament. Long-term trend: (r=.07); short-term fluctuations (r=-.38).

In Figure 7 the opposite short-term fluctuation dynamics (r=-.38) between media problem definition 'external threat(s) (security and non-security)' and parliament problem definition 'privacy violation' are visualized. This suggests that an increase in the use of problem definition 'external threat(s)' in the media substantially corresponds to a decrease in the use of problem definition 'privacy violation' in parliament. Due to the fact that for both arenas the trade-off privacy definition is still in place, these opposing dynamics actually suggest that dynamics in both arenas move into the same direction.

Comparing the dynamics between media and parliament in the exact opposite composition – i.e., media *problem definition* 'external threat(s)' compared to parliament *problem definition* 'privacy violation' – results in a medium level correlation regarding long-term trends (r=.35). As illustrated in Figure 7 however, the correlation coefficient between media and parliament with regard to short-term fluctuations is substantial (r=.60). Since the underlying *privacy definition* is still 'privacy vs. other interests', this implies that an increase in identifying privacy violation as a problem by media corresponds to an increase in

identifying ‘external threat(s)’ as problem definition in parliament. Based on the underlying privacy definition, this would in turn suggest that media and parliament actually move into opposite directions. Again taking into account only the second half of the research period (2006-2013) results in even higher short-term fluctuation correlation coefficients for both Figure 7 (r=-.67) and Figure 8 (r=.69). This again suggests that media and parliament move into the same direction whenever external threat(s) are identified as problem definition, or when parliament identifies privacy violation as problem definition. When media identify privacy violation as problem definition, however, parliament seems to move in the opposite direction.

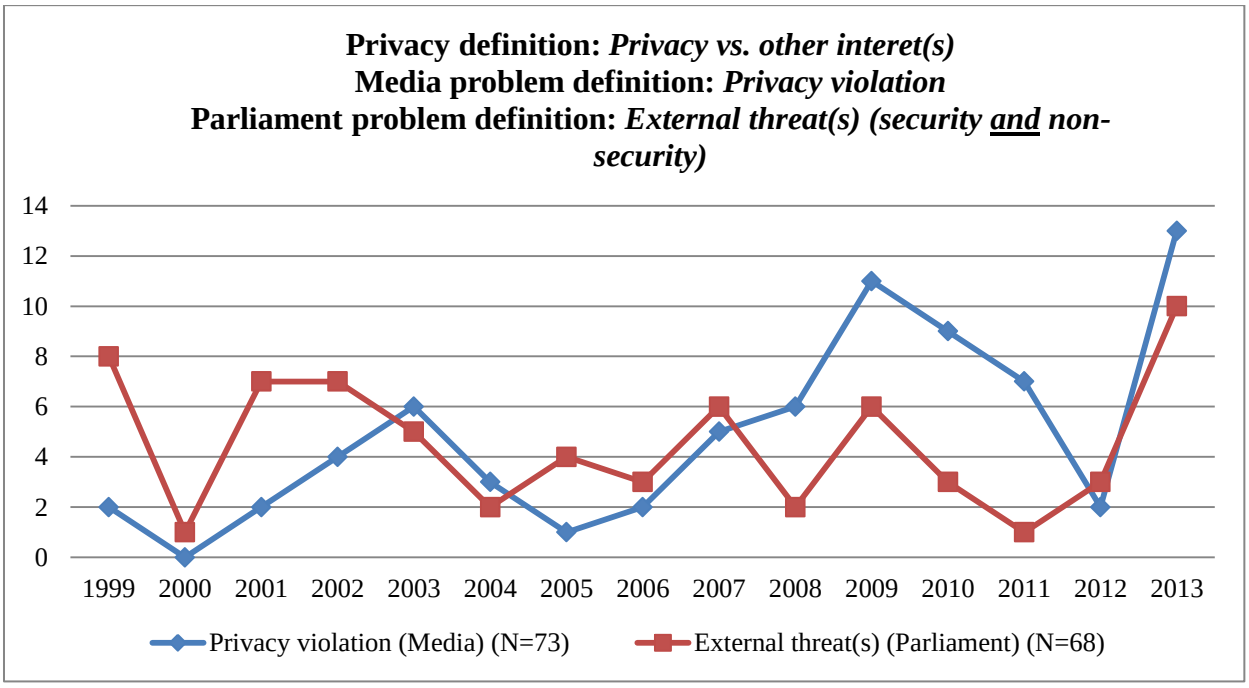

Figure 8: Comparing opposing partial-frames between media and parliament. Long-term trend: (r=.35); short-term fluctuations (r=.60).

Since both frames with regard to the role of the state are roles expected to pertain to citizens, exactly this frame component aspect is added to both partial-frames. Adding *perceived victim* ‘citizens’ threfore results in two frames, each consisting of three components. The first frame consists of privacy definition ‘privacy vs. other interests’, problem definition ‘privacy

violation' and perceived victim 'citizens', and is visualized below in Figure 9. The second frame consists of privacy definition 'privacy vs. other interests', problem definition ' external threat(s) (security and non-security) and perceived victim 'citizens', and is visualized below in Figure 10. Again, both arenas share direction in short-term fluctuations with regard to problem definition 'external threat(s)' (r=.53) and move into different direction when the problem is defined as privacy violation (r=-.38). In addition, these differences are again higher for the latter part of the research period. With regard to short term-fluctuations, Figure 9 indicates a high positive correlation coefficient for 2000-2005 (r=.76) and a substantial negative correlation coefficient for 2006-2013 (r=-.68). Figure 10 shows positive short term correlation figures throughout the whole research period. Again, however, the 2006-2013 period shows a higher short term-fluctuation correlation (r=.72) than the 2000-2005 period (r=.24).

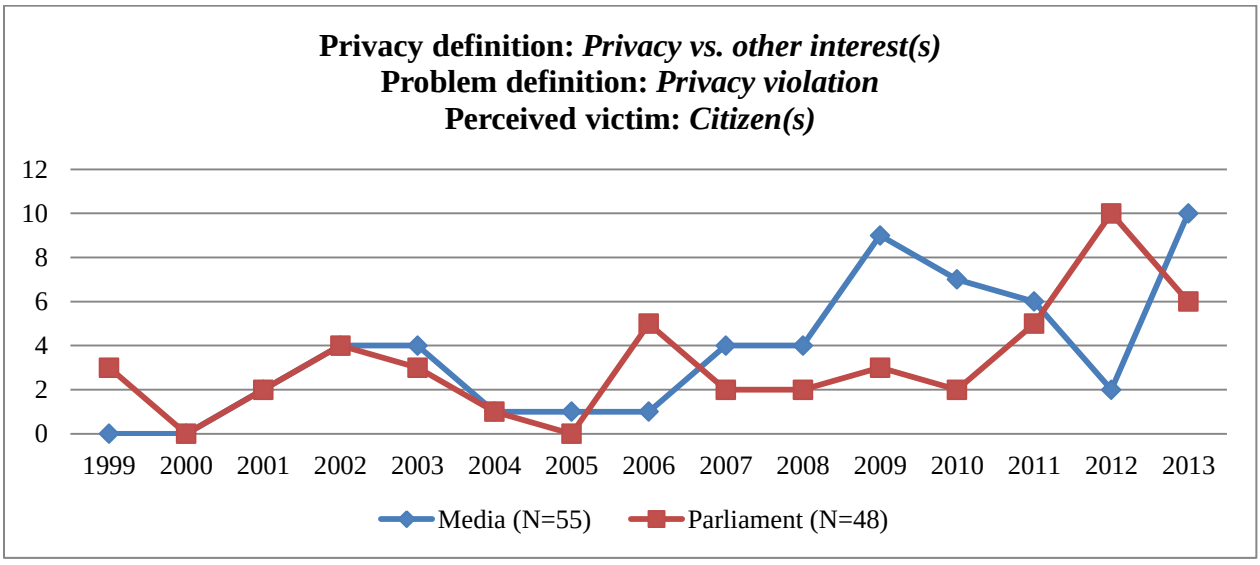

Figure 9: Comparing partial frames between media and parliament. Long-term trend: (r=.26); short-term fluctuations (r=-.38).

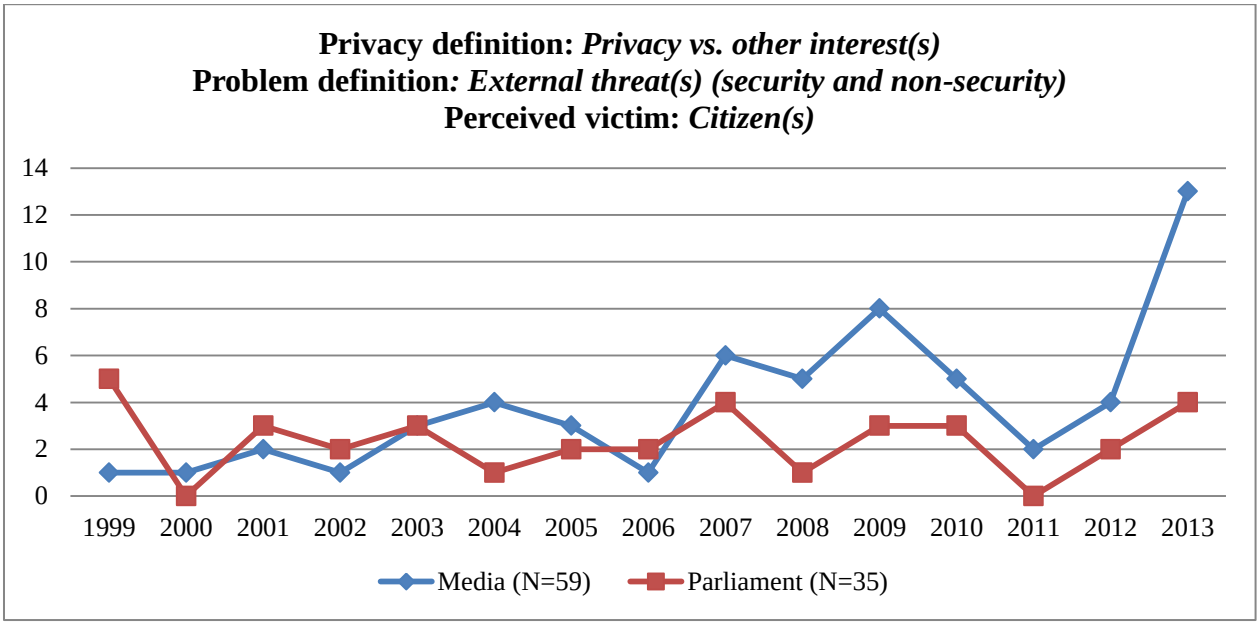

Figure 10: Comparing partial frames between media and parliament. Long-term trend (r=.37); short-term fluctuation (r=.53).

Despite these low numbers, adding this fourth component sheds light on the over-time dynamics of these frames and the differences between media and parliament with regard to framing state authorities in connection to privacy.

Frame component aspect *solution executor* ('state authorities') is added to the '*external threat(s)*' frame. In this frame the problem definition is, in contrast to figures above, defined as only 'external threat(s) (security). Leaving out the 'non-security' part better captures the nature of the hypothesis. The dynamics of this first partial-frame will be compared to the 'privacy violation' frame, to which frame component aspect *perceived perpetrator* ('state authorities') is added. Comparing these frames enables to assess the first hypothesis. Both frames are visualized in Figure 11. In this figure the frame counts in media and parliament are combined, so as to visualize the general trend.

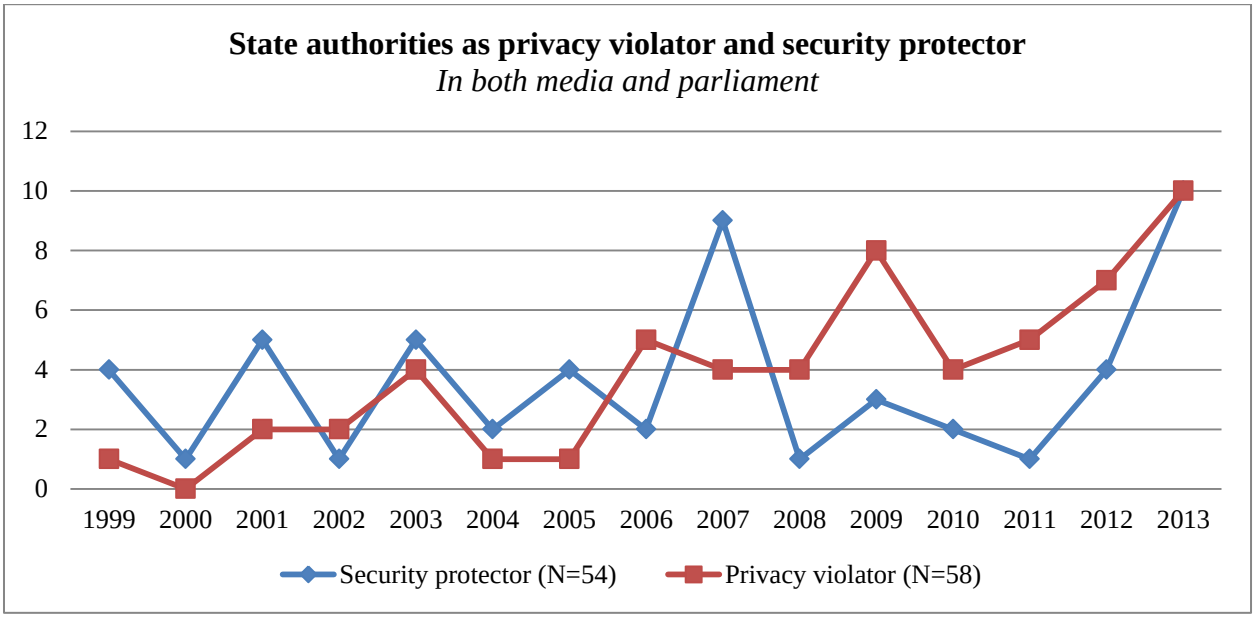

Figure 11: Comparison between partial frame 'state authorities as privacy violator' and 'security protector', visible in both media and parliament combined.

Based on this the first hypothesis outlined at the top of this section cannot fully be adopted. Although an increase in the visibility of the state-authorities-as-privacy-violators-frame is visible in the second half of the research period, it's fairer to state that both frames are used alongside the other; especially so since both frame rise to their peaks in 2013, while due to the NSA-affair the 'privacy violator' frame was expected to be more prominent. Furthermore, the expected prominence of the 'security protector' frame in the first half of the research period is not as strong as expected. This lack of visibility may be explained by the distribution of newspaper articles and parliamentary documents, which may in turn be due to the search strings that are used to collect items in both arenas. These search strings necessitate the visibility of the word 'privacy'. Since it can reasonably be assumed that in the aftermath of the 9/11 attacks substantial amounts of articles and documents on safety and security issues have been issued, these low numbers of privacy related items seem to suggest that security threats and (potential) privacy violation were not linked as much as one might retrospectively expect.

Comparing media and parliament for both these frames separately again suggests that media and parliament follow similar trends with regard to the 'security protector' frame, while on the other hand both arenas show opposing trends for the 'privacy violator' frame. The latter frame shows a low long-term trend correlation coefficient (r=.12) between media (N=35) and parliament (N=23). With regard to short-term fluctuations, the correlation coefficient is substantially negative (r=-.48). The 'security protector' frame, however, shows substantial and high correlation coefficients between media (N=32) and parliament (N=22) for long-term trend (r=.39) and short-term fluctuations (r=.61) respectively. For the second half of the research period, differences between media and parliament with regard to the visibility of both these frames are even higher. Between 2006 and 2013, the short-term fluctuation correlation coefficient between media and parliament for the 'privacy violator' frame (r=-.57) differs substantially from the period between 2000 and 2005 (r=.03). The same difference can be observed for the 'security protector' frame. The short-fluctuation correlation coefficient for this frame in the period between 2006 and 2013 is high (r=.82) as compared to a substantial correlation coefficient in the period between 2000 and 2005 (r=.42).

As mentioned above, these over-time dynamics provide only a rough indicator to assess dynamics between media and parliament. First of all, a simultaneous increase of this or any particular frame in one arena and a decrease in the other – or in fact a simultanious increase or decrease or the use of a particular frame in both arenas – does not necessarily affect the potential connection that either of these articles or documents that are present may have had with other arena.

Second, the frames elaborated are visual in connection to a multitude of events. Ideally, frame dynamics between media and parliament, or dynamics between different frames, are compared with regard to the same event. Elaborating the same event excludes the possibility of media and parliament talking past each other and provides the strongest foundation for establishing anything close to a connection between media and parliament with

regard to framing privacy. Frames regarding events within the same subject provide a surrogate for frames on actual corresponding events, since these subject are assumed to cluster relatively similar events.

In Figure 11, the peaks in 2007, 2009 and 2013 are due to the visibility of the 'security protector' frame (nineteen counts) and the 'privacy violator frame' (seventeen counts), wich together are dispersed over twenty different events. Since media and parliament are combined in this graph, the spread of these frames across several events does not tell anything about dynamics between both arenas. This suggests that the dynamics between these frames may be a coincidence since they are not connected to the samee events. What validates the comparison visualized in Figure 11, however, is the fact that all but one of the nineteen events in the peaks mentioned above are part of the privacy subject 'citizen-government'. In addition, only 2 out of all 58 visible 'privacy violator' frames and 8 out of 48 visible 'security protector' frames in Figure 11 are visible in connection to other privacy subects that 'citizen-government'. This means that, to a certain extent, the events for which both frames are visible are connected, which in turn strengthens above statements on the dynamics between both frames.

4.4 Subjects and events

Having established frame dynamics over time, distinguishing between full-frames and partial-frames, in this and following sections frames are connected to specific subjects and events. Based on Margulis (2003, 250) four different privacy subjects have been identified in the newspaper and parliamentary document selection. To these four subjects a fifth ('other') is added since multiple privacy related events, ranging from visibility in media to online privacy, are not always captured by Margulis' subjects. As visualized in 12, the most visible subject in both arenas is 'citizen-government' privacy.

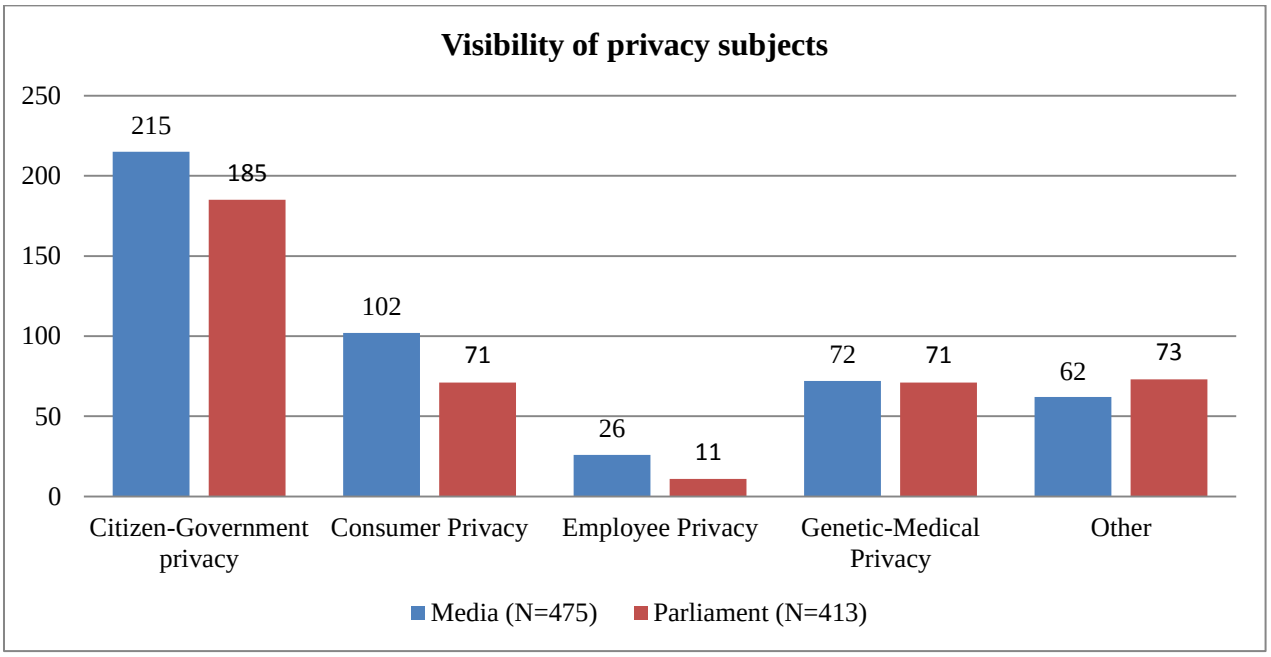

Figure 12: Visibility of privacy subjects in media and parliament

Within the article and document selection, 266 different privacy events have been identified. This is in line with the expectation that privacy is an issue connected to a wide variety of events, as outlined in the introduction. A subset of 38 events, roughly representing 14% of the total amount of events, is visible in both newspaper articles and parliamentary documents. The remaining 228 events are visible only in one of both arenas; 82 events are only visible in the media, and 146 events were only covered in parliamentary documents. The most visible

events mentioned in both arenas are 'Online privacy' (60 items), '(Electronic) Health records' (42 items) and '(Security) camera surveillance' (31 items). Other events mentioned in both media and parliament, such as ‘agreement on banking information exchange between E.U. and U.S.’ and ‘DNA test for maintenance payments’ not only appear in just a few items; these items are also at least six months apart in time, which is assumed to be too long to establish a link between media and parliament. Before focusing on mutual ‘influence’ between media and parliament, however, the second and third hypothesis will be assessed.

The second and third hypotheses are about frame dynamics between different subjects and between different events. Based on the visible aspects for frame components ‘perceived victim’, ‘perceived perpetrator’ and, to a lesser extent, ‘solution executor’, some newspaper articles and parliamentary documents on the same event are coded as representing different subjects. Although the additional ‘other’ subject has substantial counts it’s not taken into account here. This is done since it’s not part of Margulis’ typology and mainly serves as a negative category; i.e., a set of events that can not be classified as part of one of Margulis’ subjects. Taking into account only these four subjects results in 204 different visible events. As visualized in Appendix 2, 23 events are visible in more than one subject. Eighteen events are visible in two different subjects and five events are visible in three different subjects. Absence of a clear identifyable event occurs accros all four subjects.

The second hypothesis (H2) states that an increase in the use of a particular frame in one privacy subject only influences the use of frames within this particular subject. It’s basically expected that frames used in distinct groups of events ‘move’ on their own. A substantial overlap of events between different subjects would therefore suggest that the difference between these subjects is less sharp than expected; which may in turn have implications for the degree of similarity between these subjects with regard to frame dynamics. The higher the overlap, the higher similarity in frame dynamics is expected to be.

At first sight, an overlap of 23 out of 204 events seems modest. However, the events

visible in multiple subjects tend to be most visibe as well. For all 204 events, 842 frames – i.e., recorded combinations of frame component aspects – are visible throughout the entire research period[6]. Of these 842 frames, 381 are visible with regard to the 24 events that are visible in multiple subjects. This in turn seems to suggest that Margulis' privacy subjects fail to actually cluster events.

The distribution of frame counts per event across different subjects however, as visualized in Appendix 2, indicates that the bulk of counts per event is visible in one subject only. In brief, Margulis' privacy subjects are not exclusive in the sense that each subject covers a striktly confined group of events, but a rough distinction is indeed visible. Therefore, the expectation with regard to differences in framing dynamics between privacy subjects persists. In order to assess the set hypothesis, frame dynamics between different subjects will be compared. Since the frame dynamics of each these subjects are assumed to 'move' according to their own logic rather than following other subject's trends, low and (substantially) negative correlation coefficients are expected.

Because Margulis' privacy subjects are essentially distinct based on involved actors, it makes sense to asses framing dynamics between these subjects with frames based on more 'neutral' frame components only; i.e., problem definition, cause definition and solution definition. For example, comparing the dynamics of frames in which perceived victim 'patients' is visible is problematic because subject 'genetic-medical' privacy is virtually the only subject in which this frame component aspect is visible; which in turn complacates comparison. Only frame aspects that are substantially visible in multiple subjects will be used to compare frames between these subjects. Frames aspects of which the bulk is visible in one subject and the remaining counts are only remotely visible in connection to other subjects may cause (hight) positive correlation coefficients between these subjects. However, this

[6] Because frame dynamics are assessed, it's frame counts that are used throughout the analysis. The actual article count for each subject is lower. The combined amount of newspaper articles and parliamentary documents with regard to these four subjects (1999-2014) is 753; distributed across 'citizen-government privacy' (N=400), 'consumer privacy' (N=173), employee privacy' (N=37) and 'genetic-medical privacy' (N=143).

correlation would only be based on a minimal count of actual corresponding frame component aspects. In essence, this would suggest corresponding frame dynamics. However, whenever the bulk of a particular component aspect is visible in one subject, similarities are more likely to be coincidental than representations of actual corresponding frame dynamics. The only case in which similarities inframe dynamics between such subjects could be interpreted as actual corresponding frame dynamics is a situation in which the frame count of the 'bulk subject' would suddenly show a substantial peak. Such strong peaks in frame count, however, have not been established. Complete absense of any overlap in visibility of a frame component aspect would suggest that the subjects involved vary in such a way that it's not possible to compare frame dynamics between these subjects on this particular component aspect in the first place.

	Citizen-Government privacy	**Genetic-Medical Privacy**	**Consumer Privacy**	**Employee Privacy**
Privacy as control	55	63	91	8
Privacy as a (human) right	57	10	9	7
Privacy as a commodity	7	2	12	0
Privacy as a state	41	8	8	7
Privacy vs. other interests	82	20	10	6

Table 2: Countys of partial frames per privacy subject. The partial frames consist of problem defintion 'privacy violation' and one of five privacy definitions.

In absence of literature on framing privacy in media and parliament, layering frame components based on a priori expectations – i.e., identifying (partial) frames – cannot be applied in order to assess frame dynamics between privacy subjects. Besides frames reflecting a trade-off between privacy and security, the only privacy framing literature based expectation is the prominent visibility of the privacy definition 'privacy as control' (Epstein, Roth and Baumer 2014, 151).

Table 2 visualizes the counts of partial frames consisting of problem definition 'privacy violation' and one of five privacy definitions in connection to each of Margulis' four privacy subjects. This overview shows that, except for privacy subject 'employee privacy', privacy definition 'privacy as control' is substantially visible across all four privacy subjects.

The remaining partial frames, except for ‘privacy as a commodity’, seem to be most visible with regard to events related to ‘citizen-government’ privacy. Therefore, ‘Privacy as control’ is assumed to be most ‘neutral’ and used as a starting point for assessing hypothesis 2.

Comparing Margulis’ privacy subjects with regard to a partial frame consisting of privacy definition ‘privacy as control’, problem defintion ‘privacy violation’ and perceived perpetrator ‘corporate enterprises/ media/health industry’ shows ambigous dynamics. In contrast to ‘citizen-government’ privacy (N=5) and ‘employee privacy’ (N=5), both ‘genetic medical privacy’ (N=26) and ‘consumer privacy’ (N=62) show relatively substantial counts. The long-term trend correlation coefficient between these two latter subjects is low (r=.16). Short-term fluctuations show a substantial negative correlation coefficient (r=-.50). This seems to suggest that, with regard to this particular frame, privacy subjects follow their own agenda.

However, this comparison is problematic for the fact that these figures are based on the quantitative visibility of particular events. This has caused no problem with regard comparing privacy vs. security dynamics, since these frames applied to all events within one of both arenas. In that case, dissimilarities in frame counts between media and parliament could also be due to minimum visibility of particlular events in on of both arenas. This is perfectly fine, however, since the visibility of events is a prerequisite for framing connections. With regard to comparing different privacy subjects on the other hand, relying on counts is logically problematic. Dynamics between subjects with regard to the visibility of identical frames could potentially be contrary simply because for a large part each subject represents a different set of events, which may or may not be visible at certain points in time. Although not ideal, comparing percentages draws a more acurate picture of inter-subject frame dynamics.

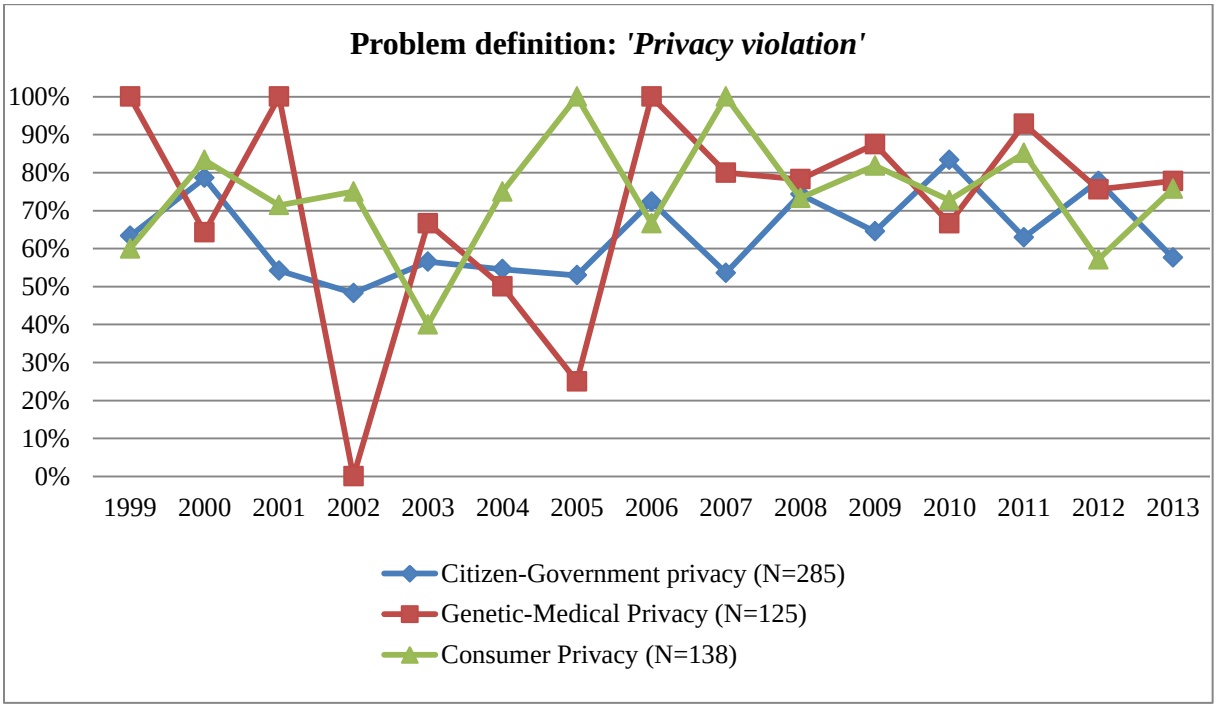

Figure 13: Percentual visibility of problem definition 'privacy violation across three privacy subjects.

Comparing the over-time percentage of particular frame component aspects within each subject sheds light on changing frame dynamics within each subject; regardless of the fact that each subject represents different events. In Figure 13, the most visible problem definition across three subjects is visualized as a percentage per year for each subject[7]. Problem definition 'privacy violation' is visible in 580 out of 842 frames (rougly 69%) within newspaper articles and parliamentary documents connected to Margulis' four privacy subjects. Regarding this frame component aspect, short-term fluctuations correlation coefficients between citizen government and genetic medical are low (r=.03). Furthermore, the short-trem correlation coefficient is substantially negative between citizen government and consumer privacy (r=-.54) and genetic medical and consumer privacy (r=-.50) respectively. These figures suggest that with regard to this single privacy component aspect, each subject follows its own logic. As shown in Appendix 3, comparing subjects with regard

[7] Privacy subject 'employee privacy' (N=32) is ignored due to substantial lower overall counts (also visible in Table X).

to other problem definitions is problematic for these lack substantial counts in more than one subject.

Building on this problem definition by adding ‘non-neutral’ frame component ‘perceived perpetrator’ results in the expected differences between subjects mentioned above. Only two pereceiver perpetrators are substantially visible. However, component aspect ‘state authorities’ is the most visible ‘perceived perpetrator’ with regard to privacy violation in privacy subject ‘citizen-government’. In other subjects however, state authorities are far less visible in this role. In contrast, perceived perpetrator ‘corporate enterprises/media/health industry’ is fairly visible across all subjects. Figure 14 therefore visualizes the share of this perceived perpetrator as a percentage of privacy violation frames per year for each subject; i.e., problem definition ‘privacy violation’ is the new baseline from which percentages are calculated.

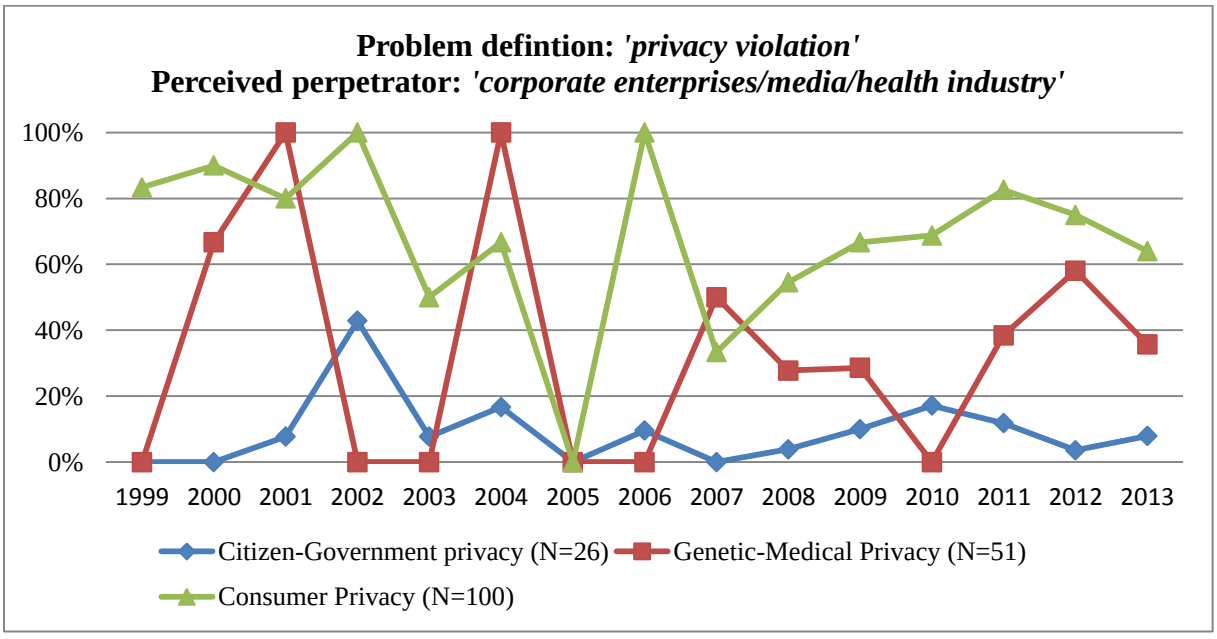

Figure 14: Percentual visibility of perceived privacy violator 'corporate enterprises/media/health industry' across three privacy subjects

Again, privacy subject employee privacy is ignored for reasons of low overall count. The ‘citizen-government’ subject shows only a few modest peaks, since the visibility of this

particular perceived privacy voilator is only little visible in this subject. The short-term fluctuations correlation coefficient between subjects ‘citizen privacy’ and ‘consumer privacy’, however, is high (r=.61). This high positive cannot be explained by an overlap in event between these subjects in 2002, 2004, 2006 and 2010. In each of these years different events have been visible with regard to each subject. This would suggest genuine corresponding frame changes between different privacy subjects. However, both subjects’ ‘peaks’ in 2004 and 2006, are really only a percentage peaks, representing actual counts of 1 and 2 frames for ‘citizen-government’ and 2 frames both years for ‘consumer privacy' respectively. The peaks in 2002 and 2004 respresent 6 frames each for subject ‘citizen government’ and 6 and 11 frames for subject ‘consumer privacy’ respectively. Therefore, these peaks run counter to the set hypothesis.

Although not every possible frame aspect combination can be assessed within the confines of this thesis, differences in substantial visibility of frame component aspects suggest that each subject has framing dynamics of its own. Remaining examples of this are frame components perceived cause and solution.

Whereas perceived cause ‘(too) far reaching of interception’ is only substantially visible in connection to subject ‘citizen government’ (N=135, roughly 77% of total visibility within these subjects), perceived cause ‘(undesired) disclosure of (personal) information’ is visible across subject ‘citizen-governmen privacy’, ‘genetic-medical privacy’ and ‘consumer privacy’.The short-term fluctuation correlation coefficient between ‘citizen-government privacy’ and ‘genetic-medical privacy’ (r=-.18) and between ‘citizen-government privacy’ and ‘consumer privacy’ (r=-.67) are moderately and highly negative respectively. The short-term fluctuation correation coefficient between ‘genetic-medical privacy’ and ‘consumer privacy’ (r=.36) is unexpectedely hight. This substatial positive correlation cannot be explained by overlap of events between both subjects. For the entire research period (with

regard to problem definition 'privacy violation') subject 'genetic-medical privacy' and 'consumer privacy' have no events in common.

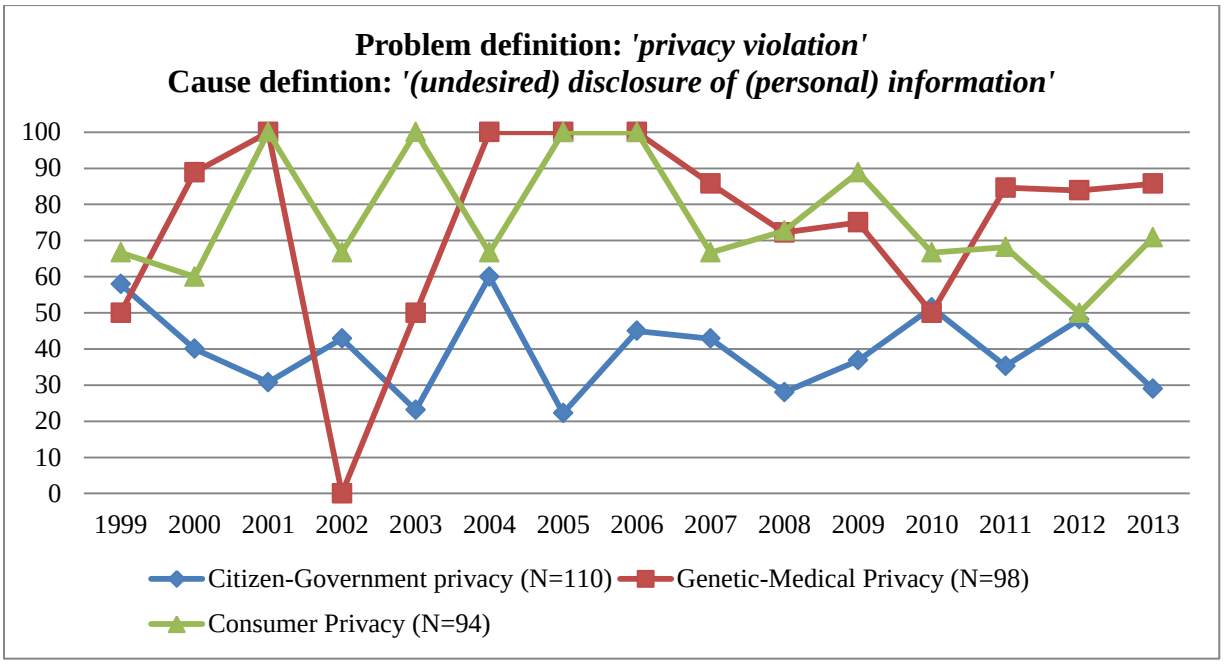

Figure 15: Percentual visibility of perceived cause of privacy violation across three privacy subjects

The last frame component that will be scrutinized with regard to inter-subject frame dynamics is 'perceived solution'. With regard to privacy violation both perceived solution '(expand) privacy protection' and 'other' are substantially visible across all four privacy subjects. Again long- and short-term correlation coefficients yield ambiguous results. With regard to '(expand) privacy protection', short-term fluctuation correlation coefficients are negative (r=.12) between 'citizen government-privacy' (N=126) and 'genetic-medical privacy' (N=41), and very low (r=.03) between 'citizen-government privacy' and 'consumer privacy' (N=56). The same figure between 'citizen government-privacy' and 'consumer privacy' is low (r=.16). This positive correlation cannot be explained by event-overlap between both subjects, for both subject (with regard to 'privacy violation') are connected to completely different events throughout the entire research period.

Regarding perceived solution ‘other’, short-term fluctuation correlation shows negative and low positive coefficients between ‘citizen-government privacy’ (N=59) and ‘consumer privacy’ (N=56) (r=-.13), and between ‘genetic-medical privacy’ (N=34) and ‘consumer privacy’ (r=.11). Contrary to proir expectations, the short-term fluctuation correlation coefficient between ‘citizen-government privacy’ and ‘genetic-medical privacy’ shows a substantial positive correlation coefficient (r=.50). Again, this figure cannot be explained by event-overlap between both these subjects. Although in this case there is overlap between both subjects with regard to events ‘(mandatory) DNA Database’, ‘(electronic) health records’ and ‘medical cofidentiality’, the total count of frames on these events, 18 out of 93 is fairly low.

Generally, it appears that frame changes between different privacy subjects don’t coincide, which suggests that each privacy subject follows its own agenda with regard to framing dynamics. Some frame component aspects turn out to be exeptions. Based, furthermore, on the fact that most frame indicator aspects seem to cluster around one subject – rather than being evenly distributed over several subjects – it can cautiously be argues that frame changes within one privacy subject only influences the use of frames within this particular subject.

The third hypothesis is about the frame dynamics between different privacy events within the same privacy subject. It states that an increase in the use of a particular frame related to one privacy event, results in an increased use of this very frame with regard to events within the same subject. The problem here is that ansrering this question necessitates long-term coverage of at least two events durigng the same period, which in turn can be compared with regard to frame changes.

4.5 Who is leading whom?

When it comes to comparing the use of frames in media and parliament, the bottom-line question is: who follows whom? Although different in wording, the first research question (RQ1) presented in this thesis asks exactly that: is media leading politics, or is politics leading media with regard to framing privacy related events? In the Figures showed above, long-term framing dynamics and short-term fluctuations have been illustrated. Although these figures shed light on the use of individual frame aspects, full-frames and partial-frames over a longer period of time, the who-follows-whom-question needs a more subtle, small scale approach. The reason for this is twofold. First, above discussed frames are dispersed over a multitude of subjects and privacy related events. As outlined above, it's expected that frames within different subjects show dynamics distinguished from other subjects. Subsequently, figures in which all subjects are taken into account may show dynamics that are unnecessary blurry.

Furthermore, correlations per year include too much time as to be able to speak of following or leading characteristics for either media or parliament. Based on the data, actual influence cannot be established; especially so since none of the references in parliamentary documents refer to items in the newspaper selection. What can be done, however, is to build a model that despite providing only yet anothorer a rough indication, provides a clearer pricture on how frame dynamics between media and parliament are structured.

4.5.1 Frame component overlap model

In order to answer this who-follows-who-question between media and parliament, only those events visible in both arenas are taken into account. Events that are only visible in either media or parliament cannot be used to analyze these between-arenas-dynamics and are therefore ignored. As mentioned earlier, this amount of events is 38. Furthermore, only those events are taken into account with regard to which at least one parliamentary document has

been preceded or followed by a newspaper article on the same event within a six month period. A period longer than six months is deemed to be too long for either a newspaper article or a parliamentary document to establish a link between both arenas. Taking this additional condition into account results in a total of 27 events.

Parliamentary documents are the starting point of analyzing media-parliament dynamics. This is done because parliamentary documents are smaller in number than newspaper articles. Each parliamentary document with regard to one of the 27 events mentioned above has been listed together with newspaper articles on the same events issued within the preceding and subsequent six month time period. Based on this list, all overlapping frame component aspects between the relevant parliamentary documents and newspaper articles have been highlighted as visualized in Figure16. This enables to calculate the average count of overlapping frame component aspects in newspaper articles preceding and following each relevant parliamentary document. This average count is between zero and seven, for there are seven frame components.

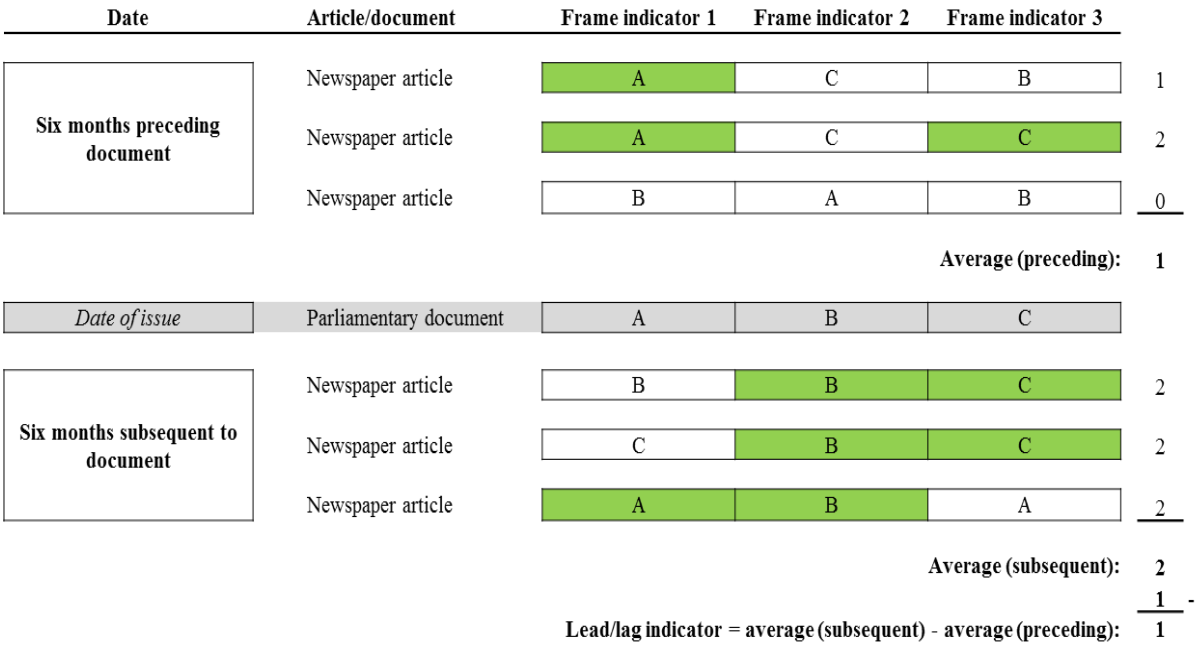

Figure 16: Hypothetical example of media-parliament model. Lead/lag indicator is 1.00 (post – pre = 2 – 1)

Figure 16 provides a simplified hypothetical example, in which the average count of overlapping frame component aspects in newspaper articles preceding the parliamentary document is 1. The average count of overlapping frame component aspects in newspaper articles following the parliamentary document is 2. The average lead/lag indicator can be calculated by subtracting the latter from the former, which in this example results in 1.

A positive average lead/lag indicator means that the average overlap of frame component aspects per newspaper article is higher for those newspaper articles following the parliamentary document than newspaper articles preceding the parliamentary document. This in turn would suggest that with regard to this parliamentary document, parliament appears to lead media in framing privacy. On the other hand, a negative average lead/lag indicator means that the average overlap of frame component aspects per newspaper article is higher for those newspaper articles preceding the parliamentary document than newspaper articles following the parliamentary document. This would suggest that rather than parliament is leading media, media is leading parliament with regard to framing privacy.

As said, in order to identify these dynamics at least one parliamentary document per event must be preceded or followed by a newspaper article within the stipulated time frame. As outlined in [Table], the count of relevant parliamentary documents per event – for the 27 events under consideration – varies between 1 ('Meta data collection' and 'Swedish interception law' among others) and 19 ('Online privacy'). The total count of relevant parliamentary documents is 97. Of the 27 events, there are 11 event with a positive lead/lag indicator. The remaining 16 events have a negative lead/lag indicator. The overall average lead/lag indicator, or ‘average mean’, is -.75. This would suggest that, on average, media is leading parliament with regard to framing privacy related issues.

	Parliamentary documents	Average lead/lag indicator
Sotsji (Olympic Games)	2	5,00
Google (streetview)	2	3,33
Record vehicle registration numbers	2	3,00
Victim's privacy	2	3,00
Swedish interception law	1	2,50
(Electronic) Performance Monitoring	2	2,09
Passing on data to state authorities (Corporate)	2	1,50
Medical confidentiality	6	0,50
Q-fever and provision of information	2	0,50
NSA/PRISM	2	0,19
Data linkage	3	0,00
Privacy of suspects	5	-0,14
(Security) Camera surveilance	6	-0,17
Electronic Health records	13	-0,65
Trade in (personal) information	5	-0,73
Online privacy	19	-1,51
Public transport chipcard	2	-2,00
Tena issue	3	-2,00
Preventative searches	1	-2,00
(Mandatory) DNA Database	1	-2,50
(Meta) Data collection	1	-2,50
Privacy of convicts	1	-2,50
Collecting airline passenger information	6	-3,33
Albert Heijn bonus card	2	-3,50
Dutch privacy level	2	-4,00
Cookies	3	-4,44
Frisking at airports (also bodyscans)	1	-5,50
Total:	97	
Average mean:	-0,75	

Table 3: Average lead/lag indicator per relevant event.

Based on the assumption that while in the aftermath of the 9/11 terrorist attacks governments were in possession of relevant information, media were in possession of relevant information with regard to Edward Snowden's revelations it's expected that over time media has become more leading with regard to framing privacy related events. When all individual lead/lag indicators (i.e., for each parliamentary document) are put in a single graph, as visualized in Figure 17, over-time dynamics regarding reciprocal 'influence' is visualized. The problem with this graph is however, that simply sorting the parliamentary documents from oldest to newest results in anything but a standard timeline. In the years 2000, 2006 and 2007 no relevant parliamentary documents were issued and the amount of relevant

parliamentary documents highly differs per year. This problem aside, Figure 17 shows no indication of a clear up- or downward trend with regard to the expected transfer of 'influence' from parliament to media. Although the trend is slightly downward, over the course of the whole research period peaks in both positive and negative lead/lag indicators are visible.

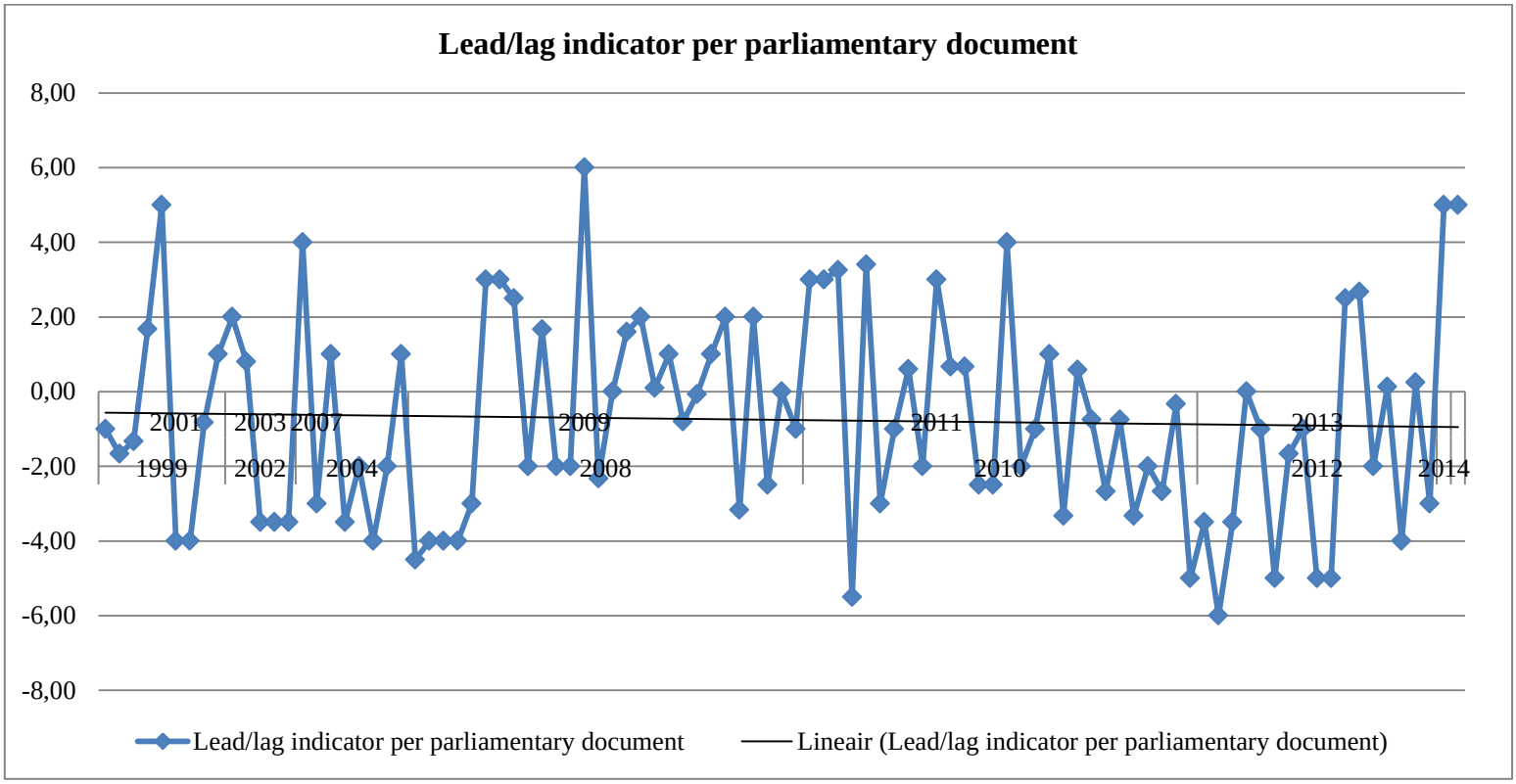

Figure 17: Over-time trend of lead/lag indicator per parliamentary document.

Potential problems with this model are twofold. First, while the average amount of overlapping frame component aspects for newspaper articles preceding and following a particular parliamentary document is equal, the actual amount of articles preceding and following the parliamentary document within six months' time may be very different. For example, one preceding newspaper article with 5 overlapping frame component aspects yields a higher average overlap than five articles following the parliamentary document with 4,4,4,5, and 6 overlapping frame component aspects respectively. In brief, the absolute count of preceding and subsequent newspaper articles is not weighted into the model. Second, the average count of overlapping frame component aspects in newspaper articles preceding and

following a particular parliamentary document may be equal, while the actual overlapping frame component aspects may be (partially) different. Subsequently, like the figures in the previous section, these results provide at best a rough indicator for answering the question which of both arenas, if at all, is leading the other.

5 Discussion

Existing framing literature has provided insight on how shaping a message may potentially influence the reader's evaluation of the particular issue at hand. According to Entman, framing can be understood as "(…) to select some aspects of a perceived reality and make them more salient in a communicating context, in such a way as to promote a particular problem definition, causal interpretation, moral evaluation, and/or treatment recommendation" (Entman 1993, 52; as quoted in Matthes and Kohring 2008, 264). The starting point for this thesis is the assumption that media and parliament influence each other in how salient issues are evaluated. This presuposes a framing relation between both arenas.

Researching this presumed relation however leaves the researcher in absense of a clear identifyable sender and receiver. First, because both media and parliament consist of multiple indipendent actors. Second, because the relation between media and parliament is anything but one-way traffic. Therefore, similarities in evaluating issues and events between both arenas cannot be traced back to a point of origin. The main research question to what extend media *influences* parliament with regard to privacy related events can therefore not be answered.

The closest surogate for influence between media and parliament may be explicit references to specific newspaper articles or parliamentary documents. These would provide the opportunity to compare source and subsequent docuement or article. The fact that non of the recorded references in parliamentary documents refer to newspaper articles within the article selection results in the impossibility of establishing a certain relation between media and parliament. Even if the exact sources were available, causal framing influence cannot be established. Corresponding frames between newspaper article and parliamentary document in conjunction with an explicit reference is highly likely to be at least partially of influence, but can never establish a unambiguous causal relation. The reason for this is that the article or

document is nothin but the packaging in which the message is wrapped; i.e., these documents are not the source. The source is an individual who may be influenced by anything but the document he's refering to. The origin of the message, and subsequently any causal relation can therefore, if at all, not be established by means of content analysis.

The lead/lag indicator that has been provided can only establish the average frame component aspecty overlap between parliamentary documents and newspaper articles. Although this indicator sheds light on these overlap figures, it has serious limitations. First, the average lead/lag indicator ignores the actual overlap count. This may result in identical prior and subsequent overlap counts while the amount of articles differs greatly. Furthermore, both the average and the acual prior and subsequent figures may de equal, this does not necessary mean that the overlapping frame components are qualitatively the same. Further research should therefore focus on the development of measurement techniques by which reciprocal dynamics between media and parliament can be measured.

6 Conclusion

This thesis tries to shed light on privacy frames in Dutch media and parliament. It compares the way in which both arenas frame state authorities with regard to privacy related events, clarifies the extend to which frame changes are incorporated across different privacy subjects and explores whether one of both arenas is leading the other with regard to framing privacy related events. With regard to the way in which state authorities are framed over time, the data seems suggests that rather than a change from framing states as security protector towards framing states as privacy violator, both frames are used alongside each other. Whenever the amount of newspaper articles and parliamentary documents increase, both frames increase simultaneously. The first hypothesis, which expects and increase in the visibility of state authorities as privacy violators at the expense of the visibility of state authorities as security protector, can therefore not be addopted.

The substantial increase in the amount of relevant newspaper articles and parliamentary documents from 2006 onwards suggests that during the latter half of the research period privacy becomes a more important issue. Since no major event has been identified halfway the research period, it may be speculated that graduate changes in information and communication technology have altered the way privacy is perceived and has led to an increase of privacy awareness in both arenas. During this period however, frames in both media and parliament appear to move in the same direction when it comes to identifying security threats as perceived problem. With regard identifying privacy violation as problem defintion, media and parliament appear to move into opposite direction. It may be speculated that based on different interest, media and parliament have different agendas when it comes to privacy. However, the assessed data cannot provide an answer to that question.

The second hypothesis concerns the effects of changes in the use of frames. It's expected that privacy subject, as distinguished by Margulish (2003), provide for clusters of privacy related events that show frame damics of their own. Based on the assessed newspaper articles and parliamentary documents this hypothesis can be addopted only cautiously. Although it's argued that lack of substanial visibility for multiple frame component aspects across multiple subjects indicates that frame dynamics differ substantially between privacy subjects, some component aspects to indicate otherwise. In contrast to the expected low and negative correlation coefficients between different privacy subjects some frame component aspects result in substantial positive correlation coefficients. As long as both subjects are constituted by different sets of events, or have only few events in common, it could be suggested that frame changes in one subject trancent to other subjects. Since the event overlap between subjects is minimal at best, these corresponding frame dynamics go against the a priori expectation.

The third and final finding in this thesis shows that both media and parliament lack clear and consistent initiative with regard to framing privacy related events. By means of the

lead/lag indicator elaborated in this thesis it’s atempted to provide a measure for answering the who-follows-who quesion. Since the relation between media and parliameny is assumed to be reciprocal a clear cut answer cannot be provided. The negative average/lead/lag indicator, which indicates that the average amount of corresponding frame components between parliamentary documents and subsequent newspaper articles is higher than between parliamentary documents and preceding articles, suggests that on average media appears to lead parliament with regard to framing privacy related events.

Literature

Babbie, Earl. 2003.
The Pratice of Social Research. Wadsworth.

BeVier. L.R. 1995.
"Information About Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection." *William & Mary Bill of Rights Journal* 4(2): 455-506.

Chong, Dennis and Druckman, James N. 2007.
"Framing Theory." *Annual Review of Political Science* 10: 103-126.

De Vreese, Claes H.; Peter, Jochen and Semetko, Holli A. 2001.
"Framing Politics at the Launch of the Euro: A Cross-National Comparative STudy of Frames in the News." *Political Communication* 18: 107-122.

De Vreese, Claes H. 2005.
"News Framing: Theory and Typology." *Document and Design* 13(1): 51-62).

Eijk, Cees van der. 2000.
"The Netherlands: Media and Politics between Segmented Pluralism and Market Forces." In *Democracy and the Media: A Comparative Persepective*, Richard Gunter and Anthony Mughan, eds. New York: Cambridge University Press, 303-342.

Entman, Robert M. 2003.
"Cascading Activation: Contesting the White House's Frame After 9/11." *Political Communication* 20: 415–432.

Entman, Robert M. 2007.
"Framing Bias: Media in the Distribution of Power." *Journal of Communication* 57: 163–173.

Epstein, Dmitry, Roth, Merrill C., & Baumer, Eric P. S. 2014.
It's the definition, stupid! Framing of online privacy in the Internet Governance Forum debates. *Journal of Information Policy* 4:144-172.

Esser, Frank; et. al. 2012.
"Political Information Opportunities in Europe: A Longitudinal and Comparative Study of Thirteen Television Systems." *The International Journal of Press/Politics* 17(3): 247-274.

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

Gitlin, T. 1980.
The Whole World is Watching. Berkeley: University of California Press.

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

Iyengar, Shanto. 1996.

"Framing Responsibility for Political Issues." *Annals of the American Academy of Political and Social Science* 546: 59-70.

Kleijnnijenhuis, J. and Rietberg, E. 1995.
Parties, Media, the Public and the Economy: Patterns of Societal Agenda-Setting. *European Journal of Political Research* 28(1): 95-118.

Lasswell, Harald D. 1948.
Power and Personality. New York.

Lewis, Justin; Williams, Andrew and Franklin, Bob. 2008.
"A Compromised Fourth Estate?" *Journalism Studies* 9(1): 1-20.

Lieshout, Marc van; Friedewald, Michael; Wright, David and Gutwirth, Serge. 2013.
"Reconciling privacy and security." *The European Journal of Social Science Research* 26(1-2) 119-132.

Margulis, Stephen, T. 1977.
"Conceptions of Privacy: Current Status and Nexts Steps," *Journal of Social Issues* 33(3):5-21.

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

Matthes, Jörg. 2009.
"What's in a Frame? A Content Analysis of Media Framing Studies in the World's Leading Communication Journals, 1990-2005." *J&MC Quarterly* 86(2): 349-367.

Matthes, Jörg and Kohring, Matthias. 2008.
"The Content snalysis of Media Frames: Toward Improving Reliability and Validity." *Journal of Communication* 58: 258-279.

Nissenbaum, Helen. 1998.
"Protecting Privacy in An Information Age: The Problem of Privacy in Public." *Law and Philosophy* 17: 559-596.

Scheufele, Dietram A. and Tewksbury, David. 2007.
"Models of media effects." *Journal of Communication* 57: 9-20.

Semetko, Holli A. and Valkenburg, Patti M. 2000.
"Framing European Politics: A content analysis of Press and Television News." *Journal of Communication* 50(2): 93-109.

Smith, H. Jeff; Dinev, Tamara and Xu, Heng. 2011.
"Information Privacy Research: An interdisciplinary Review." *MIS Quarterly* 35(4): 989-1016.

Sokora, S.N. 2002.
"Issue Attributes and Agenda-Setting by Media, the Public and Policymakers in Canada." *International Journal of Public Opinion Research* 14: 264-285.

Takeshita, Toshio. 2005.
"Current Critical Problems in Agenda-Setting Research." *International Journal of Public Opinion Research* 18(3): 275-296.

Taylor, Mark. 2012.
Genetic Data and the Law: A Critical Perspective on Privacy Protection. Cambridge University Press.

Vliegenthart, Rens and Roggeband, Conny. 2007.
"Framing Immigration and Integration." *International Communication Gazette* 69(3): 295-319.

Walgrave, Stefaan and Van Aelst, Peter. 2006.
"The Contingency of the Mass Media's Political Agenda Setting Power: Toward a Preliminary Theory." *Journal of Communication* 56: 88-109.

Westin, Alan F. 2003.
"Social and Political Dimensions of Privacy." *Journal of Social Issues* 59(2): 431-453.

Whitten-Woodring, Jenifer. 2009.
"Watchdog or Lapdog? Media Freedom, Regime Type, and Government Respect for Human Rights." *InternationalStudies Quarterly* 53(3):595-625.

Wolfsfeld, Gadi. 2011.
Making Sense of Media and Politics. Taylor & Francis.

Appendix 1: Codebook

Privacy definition

- Privacy as (a means to) freedom of expression
- Privacy as a (human) right (Also references to International Convention of Human Rights)
- Privacy as a commodity
  - (Conscious) exchange of privacy for different interest
- Privacy as a state
  - Privacy related to spying, eavesdropping and (physical) visibility related to 'state of being'
- Privacy as control
  - Privacy related to control over information, choice of exchange and being aware of threats or concessions to privacy
- Privacy equals security
- Privacy vs. [interest] *
- Privacy vs. Freedom of press*
- Privacy vs. Right to information*
- Privacy vs. Security*
- N.A.

* Unless otherwise indicated, in the analysis recoded into: *'Privacy vs. other interests'*.

Problem Definition:

- Economic consequences
  - Economic impact on businesses (also ineffective marketing), state or individual with respect to exchange or protection of privacy
- External threat(s) (non-security)
  - Non-privacy threats such as information unavailability
- External threat(s) (security)
  - Security (**not** equated with privacy), questionable effectiveness of safety measures
- Privacy violation
- Other
- N.A.

Cause definition:

- (Too) far reaching of interception **
  - Also lack of regulation
- (Too) far reaching of privacy protection
  - Infringement of other interests
- (Undesired) disclosure of information **
  - Also uncertainty about (future) application of information, also fysical
- Security threat(s)
  - (**not** equated with privacy), also inefficient investigative techniques
- Non-security threat(s)
  - Also inefficient marketing or business interests, trading in personal information
- N.A.

** Unless otherwise indicated, in the analysis recoded into: *'Interception/(undesired) disclosure'*

Perceived perpetrator:

- State authorities
  - State officials, politicians, political parties, supranational (governmental) organizations (EU).
- Terrorists/criminals/lawbreakers/individual actors
- Corporate enterprises/media/health industry
- Other
- N.A.

Perceived victim:

- Citizens
  - Also celeberties, **not** society in general
- Consumers
- Employees
- Patients
  - Also family of patients
- Crime suspects
- Society/corporate (media) interests
- Other
  - Also family of detained individuals
- N.A.

Solution definition:

- Expand privacy protection ***
  - Also constraining governmental/corporate (interception) power(s), introduce laws and regulations
  - Also prohibition of privacy infringement
- Technological fix (Expand privacy protection)
- Decrease Privacy protection ****
  - Also expand governmental/corporate (interception) power(s)
  - Also technological solutions (camera, monitoring)
  - Also monitoring behaviour
- Publish/provide (personal) information (media/individual) ****
- Don't publish/provide (personal) information (media/individual) ***
- Other
- N.A.

*** Unless otherwise indicated, in the analysis recoded into: *'(Expand) Privacy protection'*

**** Unless otherwise indicated, in the analysis recoded into: *'Decrease privacy protection'*

Solution executor:

- State authorities
- Coporate enterprises
  - Also websites, health insurance companies, media
- Judiciary
- Societal groups/individuals

Appendix 2: Subjects and (overlapping) events

		Citizen-Government	Genetic-Medical	Consumer	Employee
	Event visible in <u>two</u> subjects				
1	Multiple	**27**	-	2	-
2	Collecting airline information	**21**	-	1	-
3	Licence parking	9	-	2	-
4	Medical confidentiallity	2	**21**	-	-
5	(Mandatory) DNA Database	7	12	-	-
6	Celeberty privacy	1	2	-	-
7	Sickness absence of employees	-	2	-	2
8	Biomedical passport	**7**	1	-	-
9	Big Brother Awards	2	1	-	-
10	Unsecured website	2	1	-	-
11	Parent questionnaire	1	1	-	-
12	Google (streetview)	2	-	**11**	-
13	Trade in information	7	-	10	-
14	Customer info to government	5	-	10	-
15	(Electronic) Performance	-	-	3	**22**
16	L.I.S.	1	-	2	-
17	CBP	1	-	1	-
18	Social security law	6	-	-	2
	Event visible in <u>three</u> subjects				
1	(security) camera surveilance	**27**	-	1	2
2	Data linkage	**13**	2	2	-
3	Privacy of convicts	7	1	1	-
4	Online privacy	5	1	**57**	-
5	(Electronic) Health Records	3	**47**	-	1

This table shows frame-countsfor each event that is visible in more than one subject. The bulk of frame-countsfor each event is visible in one subject.

\

Appendix 3: Subjects and problem defintion

Citizen-governent	**1999**	**2000**	**2001**	**2002**	**2003**	**2004**	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**Total**
Economic	2	0	0	0	1	0	0	1	2	0	0	0	0	2	3	**11**
External threat(s)	2	1	6	6	3	1	3	4	1	6	6	3	3	1	8	**54**
External threat(s)	7	2	5	6	6	4	5	3	10	3	5	3	6	4	17	**86**
Other	0	0	0	2	0	0	0	0	0	0	0	1	1	1	0	**5**
Privacy violation	19	11	13	14	13	6	9	21	15	26	20	35	17	28	38	**385**

Genetic-Medical																
Economic	0	1	0	0	0	0	0	0	1	1	0	0	0	3	0	**6**
External threat(s)	0	2	0	0	0	2	2	0	1	4	1	2	0	3	1	**18**
External threat(s)	0	2	0	0	1	0	0	0	0	0	1	1	1	4	3	**13**
Other	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	**1**
Privacy violation	2	9	2	0	2	2	1	3	8	18	14	6	13	31	14	**125**

Consumer Privacy																
Economic	1	1	1	1	1	0	0	0	0	3	1	4	4	11	5	**33**
External threat(s)	3	1		1	1	1	0	0	0	0	1	1	0	1	2	**12**
External threat(s)	0	0	0	0	1	0	0	0	0	1	0	1	0	0	0	**3**
Other	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	**1**
Privacy violation	6	10	5	6	2	3	1	2	3	11	9	16	23	16	25	**138**

Employee Privacy																
Economic	3	1	1	0	0	0	0	1	2	0	0	1	0	0	3	**12**
External threat(s)	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	**2**
External threat(s)	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	**1**
Other	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**
Privacy violation	8	3	2	2	0	1	0	4	5	1	1	2	0	0	3	**32**
Total	**55**	**44**	**35**	**39**	**31**	**20**	**22**	**39**	**48**	**74**	**59**	**77**	**68**	**105**	**123**	**839***

This table shows the visibility of frame component aspects for frame component 'problem definition' in connection to each of Margulis'privacy subjects (2003, 250).

**Due to two missing values for frame component 'problem definition', this count is lower than the total amount of frame component aspect sets visible for these four subjects (N=842).*

Appendix 4: Relevant newspaper articles and coding examples

De Telegraaf (22 november 2012, p. 6)

Databank splijt meningen;
Voor- en tegenstanders liggen overhoop over belang van privacy

Margo Stols

Na 13 jaar heeft dna-onderzoek een verdachte opgeleverd in de zaak Marianne Vaatstra: de 45-jarige veeboer Jasper S., die niet eerder in beeld was bij de politie. Pleit dit voor verplichte dna-registratie voor iedereen? Tot nu toe wordt alleen dna van veroordeelden en verdachten van zware misdrijven opgeslagen in een databank. De meningen zijn verdeeld. De jastemmers zijn met 52% net in de meerderheid. Van mij mag het. Het is vreselijk als je kind is vermoord en je zo lang in onzekerheid zit over de dader.

Niet toestaan, zeggen de tegenstanders. Het is met een kanon op een mug schieten incidenteel als in de Vaatstra-zaak is afdoende en bovendien een schandelijke aantasting van de privacy. Dna verplicht afnemen is de volgende stap in het ontnemen van de privacy onder het mom van veiligheid . Big Brother is watching you.

Onzin, zeggen de jastemmers. Privacy bestaat al jaren niet meer. Men weet bijna alles al van ons. Bonuskaart, gsm, navigatie, bankpas, ga zo maar door! Privacy moet ondergeschikt zijn aan het oplossen van misdrijven, vinden de voorstanders.

Pakkans Gevraagd naar het belangrijkste voordeel van verplichte dna-registratie wordt het makkelijker kunnen identificeren van slachtoffers genoemd, bij rampen bijvoorbeeld. Maar, zeker net zo belangrijk is het sneller en vaker kunnen oplossen van misdrijven omdat de pakkans veel groter wordt. Daar gaat een preventieve werking van uit, is de verwachting. Dan denk je wel drie keer na voordat je wat flikt.

Wie niets te verbergen heeft, heeft niets te vrezen, is een veel gebruikt argument van de voorstanders. De tegenstanders zijn het daar helemaal niet mee eens. Kom niet aan met ik heb niks te verbergen, reageert iemand boos, ik ben geen misdadiger en wens ook niet zo behandeld te worden.

Bij algehele dna-registratie worden mensen al meteen neergezet als potentiële dader. Voor reeds veroordeelde criminelen is zo n registratie prima maar niet voor de gewone burger, reageren velen verontwaardigd. De kans op fouten is bovendien groot, betogen de neestemmers.

Daarnaast bestaat de vrees dat derden misbruik zullen maken van de dna-gegevens, bijvoorbeeld zorgverzekeraars, en dat ermee gemanipuleerd wordt. Je hebt een kam, haalt hem door het haar van iemand die dronken is, je pleegt een misdrijf en legt de kam op het plaats delict. Wie wordt dan als schuldige aangewezen?

Dat een dna-databank preventief werkt, zien de tegenstanders ook niet zo. Een verkrachting bijvoorbeeld is een impulsmisdrijf. Zelfs al heeft men een kilo dna opgeslagen, het zal de daad niet voorkomen.

Ruim de helft van de deelnemers heeft er weinig vertrouwen in dat de overheid zorgvuldig genoeg omgaat met dna-gegevens. Wat als de gegevens gehackt worden? De overheid heeft al eerder aangetoond slordig om te gaan met digitale bestanden. En wie is onze regering in de toekomst? Het verleden geeft het antwoord. Niet doen!

Ten slotte rest de vraag of onze samenleving er veiliger op wordt met een verplichte dna-registratie. Ook hier heerst verdeeldheid. De een ziet het als een oplossing voor een veiliger land, de ander noemt het een schijnveiligheid.

de Volkskrant (6 June 2007, p 1)

Alarm over beveiliging patiëntgegevens

Margreet Vermeulen

AMSTERDAM – Het College Bescherming Persoonsgegevens slaat alarm over de privacy van de patiënt. Door de invoering van het elektronisch patiëntendossier krijgen alle medische beroepsgroepen vanaf 2009 inzage in de patiëntendossiers. Ook in dossiers van patiënten waar ze niets mee te maken hebben. Volgens het College Bescherming Persoonsgegevens is dat 'ondenkbaar'.

In de informatie-overdracht tussen zorgverleners worden jaarlijks 1,3 miljoen fouten gemaakt, soms met fatale afloop. Het elektronisch patiëntendossier, waaraan al jaren wordt gewerkt, moet daarin verbetering brengen. Artsen, fysiotherapeuten, verpleegkundigen en andere zorgverleners kunnen dan uit het hele land snel via de computer inzage krijgen in alle medische gegevens van een patiënt.

Het College Bescherming Persoonsgegevens juicht de komst van het nieuwe systeem toe, maar vindt dat de toegang daartoe in beginsel moet worden beperkt tot zorgverleners die een behandelrelatie hebben met de patiënt. Voor andere zorgverleners moet een drempel worden ingebouwd, zodat achteraf simpel kan worden gecontroleerd of ze terecht dossiers hebben gelicht. Het college stelt dat het in strijd is met het medisch beroepsgeheim onbevoegden patiëntengegevens te laten zien.

Het ministerie van Volksgezondheid legt juist de nadruk op snelheid en gemak waarmee dossiers kunnen worden geraadpleegd als patiënten in acute nood verkeren. Het departement vreest dat een extra drempel voor gebruikers te duur wordt en ten koste gaat van de werkbaarheid van het systeem.

De Telegraaf (31 March 2009, p. 14)

“Verzet u tegen Elektronisch Patiëntendossier!”

Cees Dekker

Landelijke introductie van het EPD leidt tot schending van privacy, verkwanseling van het medisch beroepsgeheim en zal weinig meerwaarde blijken te hebben. Daarbij kost het nog eens veel geld. Zo wordt telkens gesteld door bepleiters van invoering van dit patiëntendossier dat het aantal van 19.000 vermijdbare ziekenhuisopnamen drastisch afneemt als het systeem eenmaal werkt. Die bewering is volstrekt onjuist.

De zgn. HARM-studie zegt hierover: "De frequentie van geneesmiddelgerelateerde ziekenhuisopnamen was 2,4 procent. Omgerekend naar heel Nederland betekent dit 41.000 geneesmiddelgekoppelde opnamen, en 19.000 potentieel vermijdbare opnamen per jaar." En ook: "Therapieontrouw, verminderde cognitie en nierfunctie, het niet zelfstandig wonen, meerdere aandoeningen in de medische voorgeschiedenis en polyfarmacie zijn geïdentificeerd als de belangrijkste onafhankelijke risicofactoren."

Misbruik

Allemaal factoren die niet of in beperkte mate beïnvloedbaar zijn door zo'n elektronisch dossier.

Een inbraakveilig EPD is een utopie. Het hackersonderzoek, dat de minister heeft toegezegd, heeft een groot "wij van wc-eend adviseren wc-eend!"-gehalte. Er zijn legio voorbeelden van toch niet de minste instanties die succesvol zijn gehackt, zoals het Pentagon. Vele deskundigen op het gebied van de informatie- en communicatietechnologie bevestigen de vrees en mogelijkheid dat een landelijk EPD nooit afdoende te beveiligen is. Het is niet zozeer de vraag óf dit dossier gehackt wordt, maar wanneer.

In de 22 jaar dat ik nu huisarts ben, kan ik mij geen situatie herinneren waarbij een landelijk EPD voor een van mijn patiënten meerwaarde zou hebben gehad. Ik zal mij tot het uiterste tegen deze megalomane, privacyschendende, zinloze en veel gemeenschapsgeld kostende operatie blijven verzetten.

Zou het zover komen dat deelname van huisartsen door de overheid dwingend wordt opgelegd, dan zal mij niets anders resten dan mijn werk als huisarts te staken.

Ik weiger mij een werkwijze te laten opleggen die het beroepsgeheim verkwanselt.

Als een groot deel van de huisartsen weigert aan te sluiten bij het landelijke EPD, gaat het feest niet door. In 2010 niet en later ook niet. Tot heden ben ik een gezagsgetrouw burger. Maar nu roep ik op tot burgerlijke ongehoorzaamheid. Waarde collegae: niet aansluiten, in het belang van de patiënt!

de Volkskrant (20 February 2006, p. 2)

“Waarom vertrouwen jullie de klant niet”;
Jacob Kohnstamm eist van NS zorgvuldigheid met privacy-regels bij invoering OV-chipkaart

Ferry Haan

De NS wil bij de invoering van de OV-chipkaart gegevens van de klanten opslaan. Dat is tegen de privacy-regels, vindt Jacob Kohnstamm, voorzitter van het College Bescherming Persoonsgegevens.

De Nederlandse Spoorwegen schenden de **privacy**-regels wanneer ze voor commercieel gebruik gegevens van reizigers bewaren en gebruiken. De NS is dat van plan bij de invoering van de nieuwe **OV**-chipkaart. 'De NS kan niet aantonen dat dit noodzakelijk is, dus mag het niet', stelt Jacob Kohnstamm van het College Bescherming Persoonsgegevens (CBP).

Met de **OV**-chipkaart krijgt de NS een schat aan reisgegevens en wil daar commerciële munt uit slaan. Wat is daarvan het gevaar

'Bij het CBP weten we dat we op het vinkentouw moeten zitten wanneer er sprake is van macht in combinatie met persoonsgegevens. De NS heeft macht, want het is een monopolist. Als de NS straks de reisgegevens heeft van u en mij, is het maar de vraag wat daarmee gebeurt. Zo'n bestand is geld waard. Wat gaat de NS ermee doen Gaan ze de bestanden verkopen aan commerciële partijen'

Waarom mag de NS niet weten waar ik ben geweest Mijn mobiele telefoon verraadt toch ook waar ik uithang. Die gegevens moeten zelfs wettelijk bewaard worden.

'De telefoonbedrijven mogen gegevens registreren en bewaren. Hiermee worden geschillen over rekeningen voorkomen. De telefoonbedrijven mogen deze gegevens volgens de telecomwet niet voor andere doelen gebruiken.

Voor de NS is alleen van belang dat het treinkaartje wordt betaald. Het bedrijf kan de noodzaak van het bewaren van deze gegevens niet aantonen en dus mag het niet.'

Het lijkt op de problemen destijds met de bonuskaart van Albert Heijn. Toch geven veel AH-klanten hun gegevens op.

'Albert Heijn is geen monopolist, zoals de NS. De supermarktoorlog is daarvan het bewijs. Daarbij geven de klanten hun gegevens vrijwillig. Albert Heijn heeft na enig aandringen van onze kant ook de mogelijkheid geboden de bonuskaart anoniem aan te vragen. De NS moet de klant vragen of hij zijn reisgegevens beschikbaar wil stellen. Wanneer de klant ermee instemt, is er geen enkel probleem. Ik begrijp niet waarom de NS hier niet voor kiest.'

Misschien omdat het bedrijf weet wat de klanten dan doen. Zij willen misschien niet dat de NS weet waar ze uithangen.

'Dat zeggen organisaties als de Consumentenbond, de ANWB en Rover ook. De spoorwegen zeggen dat ze met de gegevens de klant interessante aanbiedingen kunnen doen. Wanneer dat echt zo is, zal de reiziger wel toehappen. Dus, NS-directie: waarom vertrouwen jullie je klanten niet'

De NS wil de klant de mogelijkheid bieden eruit te stappen wanneer hij niet wil meedoen. Wat is daar mis mee

'Dit is de omgekeerde wereld en letterlijk 32 artikelen verder in de Wet Bescherming Persoongegevens (WBP). Wanneer de NS de noodzaak van het verzamelen van de gegevens niet kan aantonen, is er maar één mogelijkheid. De NS moet vragen aan de klant of hij ee wil meedoen. Pas wanneer de NS noodzaak kan aantonen, komt de mogelijkheid in beeld dat de klant moet vragen geschrapt te worden uit deze databestanden.'

Heeft de NS geen enkele poging gedaan de noodzaak van het bewaren van de gegevens aan te tonen

'Jawel. Ze melden ons dat ze teruggave van geld voor kaartjes automatisch willen regelen wanneer treinen vertraagd zijn. Dat moet nu via allerlei ingewikkelde formulieren en er zou misbruik van gemaakt worden. Dus hebben wij gevraagd aan de NS hoe groot dat misbruik is. Voor het bewaren van gegevens moet wettelijk worden vastgesteld dat het middel 'proportioneel' is. De NS kan dit niet en dus geven wij geen toestemming.'

De Telegraaf (31 January 2011, p. 3)

Dubbel slot op medisch dossier; Patiënt maakt uit wie gegevens mag zien

Edwin van der Aa

Patiënten mogen vanaf de lente zelf gaan bepalen welke arts of zorginstelling toegang krijgt tot hun medische gegevens. Dit zogeheten 'dubbel slot' moet de privacy van burgers beter garanderen.

Dat maakt minister Schippers (Volksgezondheid) vandaag bekend. Ook wil de bewindsvrouw ervoor zorgen dat burgers desgewenst automatisch een melding per e-mail of sms krijgen wanneer persoonlijke data via het zogeheten elektronisch patiëntendossier (EPD) worden ingezien.

"Voor mij staan de patiëntveiligheid en het voorkomen van vermijdbare medische fouten voorop", legt Schippers uit. "Maar ik heb ook oog voor gevoeligheden met betrekking tot privacy en hecht zeer aan adequate informatiebeveiliging."

Via deze maatregelen neemt Schippers een belangrijke stap om de maandenlange politieke patstelling over een verantwoorde uitvoering van het EPD te doorbreken. Tot opluchting van de zorgwereld: instellingen hebben al miljoenen geïnvesteerd in de benodigde ict-toepassingen.

Bezwaar

Op dit moment kunnen via het EPD de medische gegevens van ruim 5,8 miljoen burgers worden geraadpleegd. Sinds de landelijke campagne van 2008, waarin mensen er attent op werden gemaakt dat ze bezwaar kunnen aantekenen tegen uitwisseling, heeft 2,6% dat ook gedaan.

Experts en ingehuurde hackers hebben al verschillende 'indringerstesten' op het systeem uitgevoerd en er zaten volgens het ministerie geen grote gaten in de software. Er komt nog een grote test.

Verder wil de minister dat patiënten via de website van de eigen zorgverlener hun EPD kunnen inzien, in plaats van via een landelijk portaal.

VVD-Kamerlid Mulder laat weten het een goed idee te vinden dat de minister patiënten zelf de regie geeft over hun EPD. "Zo gaan mensen zich verantwoordelijk voelen en tegenspraak geven aan artsen."

De Telegraaf (8 September 2012, p. 27)

Webzoeker GX staat vlak voor doorbraak in VS

-

Consumenten hechten steeds minder aan volledige privacy op internet. Dat opent deuren voor bedrijven die met deze persoonlijke zoekgegevens mensen steeds meer aanbiedingen naar hun smaak doen. Met elke klik op internet worden websites persoonlijker op hen toegesneden. Het Nederlandse GX Software staat daarin voor een doorbraak.

Voor elk technologiebedrijf is de vermelding door marktonderzoeker Gartner als visionair het ultieme resultaat. De hele sector volgt dergelijke bedrijven als de meest kansrijke investeringen in komende jaren. GX Software met zijn webvolgtechnologie van consumenten is door Gartner nu als eerste Nederlandse bedrijf, naast reuzen als IBM, Microsoft, Adobe en Oracle tot die top bestempeld.

Waar steeds meer consumenten zich online laten volgen en privacy minder belangrijk vinden in ruil voor snelle digitale hulp, kan GX met elke klik steeds persoonlijker websites rond hen kneden

de Volkskrant (2 October 2001, p. 7)

Privacy verdient ook na 11 september bescherming

Anne-Marie Kemna

Beknotting van burgerrechten om terrorisme te bestrijden mag dan sinds 11 september populairder zijn geworden, maar volgens Anne-Marie Kemna is het de verkeerde weg. Inlichtingendiensten en politie zouden meer moeten doen met de bevoegdheden die ze nu al hebben.

BESCHERMING van persoonsgegevens en van de persoonlijke levenssfeer dreigt een luxegoed te worden. De dreiging die sinds lang van terroristische acties uitgaat, is werkelijkheid geworden. Een minstens zo grote bedreiging kan er ontstaan door de rechtsstaat zelf. Terrorisme en georganiseerde criminaliteit leveren zoveel angst en potentiele schade op, dat de bestrijding ervan kennelijk ten koste mag gaan van burgerrechten. Maar waar leggen we de grens?

Leveren voorgestelde maatregelen tot vergroting van de afluister-, aftap- en controlemogelijkheden niet slechts de schijn van absolute veiligheid - halen we het Paard van Troje binnen in het huis van de burgerrechten? In de VS werd twee dagen na de ramp een wetsvoorstel door de Senaat geloodst om de overheid meer mogelijkheden te geven tot informatiegaring en aftappen van telefoons. In Europa wordt druk overleg gepleegd door regeringsleiders. Uit een intern document van de Europese Commissie bleek dat een van de agendapunten is het met spoed nagaan waar nationale wetgeving ter bescherming van persoonsgegevens een belemmering vormt voor onderzoek naar terrorisme en criminaliteit.

De Telegraaf (27 November 2013, p. 9)

Fiscus mag niet altijd snuffelen;
Rechter fluit overijverige Belastingdienst terug

-

Al veertig jaar oude bevoegdheden van de Belastingdienst om bij bedrijven gegevens van burgers op te vragen moeten worden herzien. De voorzieningenrechter in Den Bosch vindt dat door de grote hoeveelheid tegenwoordig opgeslagen gegevens de privacy in het geding is.

De rechter besloot met die argumentatie dat de fiscus geen toegang krijgt tot de gegevens van klanten van parkeerbedrijf SMSParking. De Belastingsdienst wilde de gegevens om vooral lease-gebruikers van de dienst te kunnen controleren. SMSParking biedt klanten aan om overal te parkeren en dan via een sms te betalen.

De fiscus vindt dat het recht heeft op de gegevens op basis van een uitspraak van de Hoge Raad in 1974 die later door andere rechters steeds is bevestigd. Door dat veertig jaar oude arrest beschikt de fiscus over ruime bevoegdheden om informatie te krijgen.

Privacy Ik had geen zin om daar aan mee te werken , zegt Mladen Ciric van SMSParking. Volgens de fiscus moest ik die gegevens verstrekken, maar ik had er geen goed gevoel bij. Het tast de privacy van mijn klanten aan. De Belastingdienst gebruikt zo een sleepnetmethode. Ze pakken alles en kijken vervolgens of er iets bruikbaars tussen zit. Dat vind ik gewoon niet kloppen.

De fiscus spande daarop een kort geding aan, maar de rechter gaf Ciric gisteren gelijk. Volgens de rechter mogen burgers alleen om zwaarwegende redenen in hun privéleven aangetast worden.

de Volkskrant (**21 februari 2014)**

“Ik dacht direct: weg ermee!”

Het wantrouwen tegen Facebook en zijn privacybeleid is groot. Bij deskundigen en bij gebruikers van WhatsApp.

Tim Toornvliet namens privacy-organisatie Bits of Freedom:

'Ik vind het een zorgelijke overname. Facebook is een bedrijf dat onderdeel wil zijn van al je onlineactiviteiten, maar heeft tegelijkertijd een slechte reputatie op het gebied van privacy. En nu hebben ze in één klap toegang tot nog meer privégegevens. Het belangrijkste verschil zit, denk ik, in het type contact dat je hebt op beide netwerken. Op WhatsApp is dat toch een stuk intiemer. Die informatie is voor Facebook blijkbaar veel waard.'

Jaap-Henk Hoepman van het Privacy en Identity Lab van de Radboud Universiteit:

'De inhoud van de gesprekken, waar je dus precies over chat met je vrienden, is heel interessant voor Facebook. Dat is voor hen een manier om inzicht te krijgen in wat er precies speelt. Kijk naar Twitter en wat zij doen met hun zogenoemde trending topics. Die informatie verkopen ze door aan bedrijven. Het zou zomaar kunnen dat Facebook dat nu ook gaat doen.'

Internetondernemer Alexander Klöpping:

'Die angst voor één commerciële macht die praktisch al onze gegevens heeft, begrijp ik wel. Ook ik vind die consolidatie een groot probleem. Toch wil ik een belangrijk nuanceverschil maken. Privéconversaties op WhatsApp waren nooit echt privé. Je kon altijd relatief eenvoudig meelezen met de gesprekken van je buurman. Het is in die zin te vergelijken met een ansichtkaart. Ook daar staat alles open en bloot op neergekrabbeld. Wat dat betreft verbetert de situatie nu dus eigenlijk. Facebook heeft namelijk een veel groter beveiligingsteam.'

Hoepman:

'Een andere belangrijke vraag die ik heb: wat gebeurt er straks met de mobiele-telefoonnummers waartoe WhatsApp toegang heeft? Ik heb contacten in mijn lijst staan die hun telefoonnummer liever privé houden. Maar die controle is nu weg. Als jouw zoon, collega of vriendin zowel jouw nummer als WhatsApp heeft, dan heeft Facebook dat nu ook. En de gegevens zijn al verkocht dus als je nu stopt met WhatsApp, is het eigenlijk al te laat.'

Een voormalig WhatsApp-gebruikster :

'Eén ding vooraf: ik wil niet met mijn voor- en achternaam in de krant. Waarom niet? Ik vind privacy heel erg belangrijk. Daarom niet. En ja, dat is ook de reden dat ik meteen Whats-App verwijderde toen in het nieuws hoorde. De deal was nog niets eens rond en ik dacht al: hoppatee, weg ermee.

'Deze overname voelt namelijk als een klap in mijn gezicht. Waarom geef je Facebook nou ook nog mijn telefoonnummer? Dat wil ik helemaal niet. Ik heb al wel gekeken naar alternatieve applicaties zoals Viber en Telegram, want ik wil ook geen sociale paria worden.'

Klöpping:

'Er is een hele reeks aan alternatieve gespreksapps, maar uiteindelijk zijn die allemaal van bedrijven die data willen verzamelen. Allemaal. Als je nu dus overstapt naar een andere app, blijft het de vraag hoe veilig je informatie is.

'Telegram bijvoorbeeld - daar wordt nu veel over gesproken - is een app van de Russische Facebookoprichter. Tja, dan ga je dus weg bij WhatsApp omdat je Facebook niet vertrouwt, maar dan stap je over naar een andere Facebookoprichter. Ik weet het niet.'