Public Management Challenges in the Digital Risk Society

A Critical Analysis of the Public Debate on Implementation of the Danish NemID

Ngwenyama, Ojelanki; Zinner Henriksen, Helle; Hardt, Daniel

Document Version
Accepted author manuscript

Published in:
European Journal of Information Systems

DOI:
10.1080/0960085x.2021.1907234

Publication date:
2023

License
Unspecified

Citation for published version (APA):
Ngwenyama, O., Zinner Henriksen, H., & Hardt, D. (2023). Public Management Challenges in the Digital Risk Society: A Critical Analysis of the Public Debate on Implementation of the Danish NemID. *European Journal of Information Systems*, *32*(2), 108-126. https://doi.org/10.1080/0960085x.2021.1907234

PUBLIC MANAGEMENT CHALLENGES IN THE DIGITALIZATION OF SOCIETY:
A Critical Analysis of the Public Debate on Implementation of the Danish NemID

Ojelanki Ngwenyama
Helle Zinner Henriksen
Daniel Hardt

Abstract: The rise of the digital society is accompanied by incalculable social risks, but very little IS research has examined the implications of the new digital society. Drawing on concepts from Beck's critical theory of the risk society and critical discourse analysis this study examines the public discourse on risk events during the launch of NemID, a personal digital identifier for Danish citizens. This research illustrates our difficulties and challenges in managing some of the fundamental social risks from societal digitalization. Limited institutional capabilities for digital technologies force public officials to depend on private companies motived by profit instead of the public interest. Beliefs in digital technology as the primary determinant of social and economic progress also present many public management dilemmas. When digital risk events occur and citizens' fears are stoked by news media and public discourse, public officials seem to have no other strategy for managing the escalating fears than systematically distorted communication. The continued rise of the digital risk society demands that IS research respond to the challenge of generating knowledge for its public management.

Keywords: Critical social theory, digital risk society, critical IS research, national digital infrastructure.

Introduction

The last half of the twentieth century witnessed a profound digital transformation of social life. Governments are increasingly imposing digital systems to routinize public services and social interactions with citizens (Irani *et al.*, 2007; Corydon, Ganesan, Lundqvist, 2016). Some researchers have raised concerns that this digital by default approach to e-government imposed on citizens can be dehumanizing and alienating (Chandler, 2019; Berger, 2015). Furthermore, the "digital first" paradigm (Baskerville *et al.*, 2020) where digital infrastructure are deployed without adequate understanding the social risks exposes citizens and society to unknown potential harm. The digitalization of social and economic interactions has resulted in the quantum escalation of digital risks that is challenging our capabilities for managing them (Chung, 2011; Rowe, 2018). As Luhmann (2005) noted, social risks when poorly managed can undermine citizens reflexive trust, the basis for rational action and the glue holding complex societies together. In democratic societies, citizens expect public officials to manage *the affairs of state*, specifically, social risks in order to maintain social life. However, the continued digitalization of society is escalating digital risks and challenging our institutional capabilities for managing society (Curran, 2018; Hemphill & Longstreet, 2016). Every new digitalization project brings with it unpredictable and incalculable risks to citizens and society (Misuraca, Pasi, & Viscusi, 2018; Robinson, 2018). Furthermore, when digital risk events occur, they are amplified by press reports and citizen responses reproduce a climate of fear and anxiety (Chung, 2011; Gerber & Von Solms, 2005). Citizens expect government officials to project confidence that 'the situation is under control' to assuage their fears of the unpredictable and cascading consequences of the risk events (Albahar, 2017; Allen & Peloza, 2015). Public officials, who must rapidly respond to digital risk events, are often incapable of apprehending their complexity, and are dependent upon equally uninformed experts. And as Chandler (2019) noted, when reality seems too complex, public officials tend to focus on managing effects instead of searching for causal explanations upon which effective intervention can be based. While there is a body of research on risk communication to guide public health and natural disaster officials (cf. Lundgren & McMakin, 2018), there is not yet a research literature on the emerging problem of digital risk communication.

This research responds to calls for critical qualitative IS research on emerging problems from the aggressive digitalization of society (Rowe, 2018; Cecez-Kecmanovic et. al., 2020). Our focus here is on developing an understanding of the communication challenges that officials face when confronting digital risk events that have the potential to instill fear and anxiety in citizens and undermine trust in societal institutions. Our interest is developing a *theory of the problem* (Majchrzak, Markus, & Wareham, 2016), that could help advance IS research on effective digital risk communication. The *theory of the problem* is a substantive definition of the problem space, a first step toward developing a *theory of the solution* (Majchrzak, Markus, & Wareham 2016). Moreover, both *theory of the problem* and *theory of the solution* "are distinct from theories of a phenomenon (such as technology use, computer mediated communication, or IT governance) because they make explicit value judgments that the situation is problematic from the perspective of certain stakeholders and needs to

be improved" (ibid pp. 271). In this paper we set out to develop a substantive definition of the problem space; laying out its contours and core issues. In this regard, we focus on understanding and describing the dynamics of public discourse on digital risk events which have the potential to cause societal harm and instill fear in citizens. In the emerging digital risk society, digital risk events (denial of service, infodemics, data breaches) are complex and formidable challenges for public officials who are expected to manage risks to public digital infrastructures and protect citizens and democratic institutions. When such events occur information is limited, vague and unreliable. Consequently, officials make public statements that must be revised again and again as new information is revealed. Such revisions can erode public trust, as citizens get the impression that officials lack appreciation of the scale and complexity of the risk events, and cannot effectively manage them. While IS research has focused on e-government implementation, and the importance of public management of digital risks to society is now recognized (Chan, et. al., 2011; Brown & Osborne, 2013), there is scant research on this topic (Wirtz & Weyerer, 2017; Gimpel & Schmied, 2019). Using the concept of the '*world risk society*' (Beck, 2009), we take a critical social theory approach (Myers & Klein, 2011), to interrogate a set of risks events that emerged during the implementation of a mandatory personal digital identifier (NemID) in Denmark. The rest of the paper is organized as follows: We discuss prior research on media discourses on the digitalization of society. We outline the basic concepts of the *world risk society*, the critical theory perspective of our research. We then summarize the principles of our critical theory method, followed by our empirical analysis and findings. Finally, we present a theoretical discussion of the findings and conclusions.

Media Discourse and Digitalization

The news media plays an important role in the public communication and management of risk events in society (Opperhuizen, Pagiotti & Eshuis, 2020). However, there is scant research on the role of media and public discourse in shaping perceptions of the digitalization of society (Cukier, Ngwenyama, Bauer, & Middleton, 2009; Hepp, Alpen & Simon, 2020; Rowe, Ngwenyama & Richet, 2020). While digital technologies are a transformative force in society, research on how news media represent them and how we respond to those representations is limited. A few studies have identified the significance of public discourse and news media reports on shaping citizens' perceptions, understanding and expectations of digital technologies (Stahl, 1995; Olsson, 2006; Yildiz & Saylam, 2013). Digital technology is been presented with hyperbole of magic and beyond human comprehension (Stahl, 1995), a magical force for social and political progress (Kvasny and Truex, 2001), and a shortcut to civic participation (Olsson, 2006). These images influence our perceptions of digital commerce, digital democracy and the digital society (Gil de Zúñiga, Veenstra, Vraga, & Shah, 2010). Researchers also support the view that the news media carries the legitimacy of a trusted institution of society and, therefore, plays a pivotal role in shaping public opinions about issues of general concern (Myers, 1994; Williams & Edge, 1996). Furthermore, as Gamson & Modigliani (1989) pointed out, journalistic stories tend to have more influence on citizens, decision-

makers and government officials than professional technology and specialist publications.

A second set of relevant studies examined parliamentary debates and how citizen engagement in public debate about ICT public policy influenced decision making. Whitley and Hosein (2005) examined UK parliamentary debates on the UK government's proposal for a new data retention law (in the wake the US Patriot Act) that would legalize the collection of data concerning communication among UK citizens. This study is noteworthy for two reasons: (1) its critical interrogation of parliamentary debates and, (2) its exposure of challenges of balancing the interests of private citizens when enact legislation on complex and malleable digital technologies for state security in democratic societies. In another study, Whitley and Hosein (2008) reported on how engagement in public discourse by an academic institution influenced the UK government's decision to abandon a national digital identity card. An important finding of this study, which is relevant to our work, is the power of IS academics to influence public debate and policy on the trajectory of digitalization in a democratic society. A study by Cukier et al. (2009) illustrated how a set of powerful actors (public university administrators, computer and software vendors) used distorted communication to dominate the public discourse between 1994 to 2005 and to achieve citizen support and favorable government decisions to implement costly learning technologies in Canadian universities. A more recent critical theory study (Rowe, et. al., 2020) examined the impact of French parliamentary debates on the design and implementation of a StopCovid contract tracing app and their societal consequences. Our study builds upon and extends this growing body of critical theory information systems research by incorporating concepts of the *world risk society* proposed by Beck (2009).

Theoretical Framework of Research

Beck (2009) defines the *world risk society*, as "a society increasingly confronted with the undesired side effects of successful modernization". Beck's central concern are the incalculable ecological risks to global society from technology innovations (chemical, biological, industrial, nuclear) for economic advancement in modern societies. Powerful corporate actors take risks with all types of technologies (chemical, biological, industrial, nuclear, digital) for wealth generation, but are unwilling to bear the costs for consequences (Beck, 2006; Kane, 2010). Consequently, we live in imminent danger of air pollution, nuclear accidents, oil spills, water contamination from mining, climate change, etc. resulting from use of these technologies (Beck 1992b; 2009). Beck argues, that in an interconnected world, nation states can no longer control their exposure to risks of ecological and climate catastrophes resulting from the intensive use of industrial technologies (Beck, 1992b, 2015). And while rich nations get richer, poor ones get poorer and inequality expands everywhere (Beck, 2006, 2013). In the *risk society*, citizens' belief in institutional control collapses, as rules for assigning liability and responsibility are no longer effective. In an interview with Yates (2003), Beck argues, a defining feature of the *world risk society* is 'non-quantitative uncertainties enforced by rapid technological innovations.' Governments incentivize

technology risk taking for wealth building and are reluctant to regulate risk behaviors of corporate actors until crises emerge (Beck, 2006; Lazonick & Mazzucato, 2013). Beck (2009; 1992b) identifies two important characteristics of the *world risk society*: (a) risks are socially constructed and reproduced by mass media communication networks; (b) fear and anxiety of anticipated catastrophes from new technologies are constant companions of its citizens. The risks are invisible, uncontrollable, and unprecedented in geographic reach with incalculable consequences (Beck, 2006). They transform our living conditions and our relationships to social institutions, resulting in a culture of uncertainty increasingly characterized by widespread distrust in social institutions (Beck, 1992a).

The social construction of digital risks is a complex and recursive process in which claims are posited, contested and defended by powerful stakeholders resulting in temporal meanings and contingent actions (Beck, 1992a). When a risk event occurs, its significance is not immediately perceived by citizens until they experience its harmful effects or the media or other actors inform them of potential harm (Beck, 1992a; Chung, 2011). In the absence of public accounts given by the media, scientists and public officials, citizens often lack the knowledge to interpret what a risk event means and what consequences it might have for them (Luhmann, 2005; Russell & Babrow, 2011). According to Cottle (1998, p. 8), "*risks only become visible when socially defined within knowledge or knowledge processing fora such as science, the legal system and the mass media*". Moreover, public discourse of risk events is not clear cut, but entail vociferous debates in which influential stakeholders posit competing claims in support of their interests (Beck, 1992a). In democratic societies, there is a reflexive view of the media as the *fourth estate*, that mediates public discourse and enforce stakeholder accountability. In this view the media is equated with the institution of science, and is expected to be truth seeking and orientated to rational critique in defence of society. But, as Habermas (1991, 2006) has pointed out, colonization of the media by corporate and sectarian interests has undermined its legitimacy in truth seeking and rational critique. The media is not a 'neutral mediator' of public debates, it determines which scientists, public officials or citizen groups gets a voice and which perspectives of an issue are amplified or silenced (Dunwoody, 1992; Roslyng & Eskjær, 2017). While citizens depend upon the media to understand risk events, the media has power to influence the meanings they construct of such risk events and how they respond to them (Cottle, 1998; Hornig 1993). Media narratives can influence whether we respond to risk events with deliberative rational action or fear and irrationality (Innes, 2010; Altheide, 2013; Simonov, et al., 2020). Moreover, public institutions often lack resources for independent communication campaigns to promote accurate information or combat misinformation about risk events and must depend on the media (Beck, 1992b; Ungar, 2001). Hence, the media with its network power to magnify, dramatize or minimize, can transform our perceptions of risk events "*to the extent that they are open to social definition and construction"* (Beck, 1992a, p. 22). Consequently, Beck repeatedly emphasizes ***critical inquiry into public discourse processes as essential to understanding the dynamics of the risk society*** (1992a, 2006, 2009). Finally, while Beck did not address

digital risks, Lupton (2016) argues that his conceptual framework still has the potential to inform critical analysis of the emerging digital risk society.

Public Management Communication Challenges

Cyber-attacks on e-government infrastructures are a class of risks with potential to cause significant social and economic harm to society. In this regard, public officials are expected to intervene and manage the damage. They must communicate with concerned stakeholders, project confidence to build trust and credibility, while mobilizing for action and accountability (Coombs, 2014). Crisis communication researchers advise officials that truthfulness and avoidance of spin are essential for building credibility with stakeholders (Coombs & Holladay, 2002; Clementson, 2020). However, details of emerging digital risk events are usually scarce, while the scale and complexity of a risk event and its potential social and economic impact are often unknown (Chakravartty & Schiller, 2011). Public officials must depend on scientists and IT experts for information, who also lack detailed knowledge and need time to investigate the risk situation (Brunk, 2006). While public officials might feel pressured 'to get out in front' of the crisis, communicating with incomplete knowledge can lead to contradictions, revisions and retractions. Stakeholders can perceive these failures of communication as betrayals which can undermine their belief government institutions (Ma, 2018). Another challenge that public officials face in the context of digital risk events is infodemics, in which rumors and fake news about a risk event is propagated over social media stoking fear (Roozenbeek, & Van Der Linden, 2019). Concurrently, news and social media stories can amplify fears and anxiety among citizens, mobilizing more intense civic response (Chung, 2011). Beck (1997) argues that media (and public relations experts) present challenges for public management of crises, as these powerful stakeholders can define and shape our perceptions of risks, and broadcast 'risk narratives' that cultivate shared experiences of uncertainty among citizens. Scientists too, can intentionally and unintentionally contribute to the escalation of risks perceptions and fear by using opaque and indecisive language (Beck, 1992a). Furthermore, depending on their agendas, stakeholders may adopt communication strategies to facilitate shared understanding, or resort to manipulation to achieve personal goals (Habermas, 1984). Navigating public discourse on risk events and their social impacts requires adroit action from public officials to avoid panic and disruptions of social order and achieve optimal outcomes for resolving the risks (Ungar, 2001; Slovic, 1993).

Research Methodology

As stated earlier the focus of this research is developing a *theory of the problem,* i.e., 'an argument specifying relationships among conceptual elements of the problem…… that does not gloss over conflicts of values and beliefs but specifies the role of divergent perspectives in the problem situation' (Majchrzak, Markus, & Wareham, 2016; pp. 271). In this regard, the research methodology strategy is a two-phase process: (1) a

critical descriptive analysis of the discourse, followed by (2) a theoretical redescription of the empirical findings of descriptive analysis. ***Critical descriptive analysis***: For this phase we use a critical discourse analysis (CDA) method (Cukier, Ngwenyama, Bauer, & Middleton, 2009) to interrogate the public discourse on risk events on the NemID infrastructure in Denmark. The CDA involves: (1) identifying and assembling relevant materials of the discourse; (2) identifying the key stakeholders and key events of the discourse; and (3) critically analyzing the discourse. An important issue in any longitudinal research is capturing the appropriate time horizon (Street & Ward, 2012). In this case we set the frame 1½ years prior and 4 years after implementation to capture the full discourse. Using the term "NemID" we searched the Infomedia Archive© for the 2009 and mid-2014 and got 936 unique items from the six national Danish newspapers and two tabloids. For CDA of the empirical materials we employed qualitative (NVivo), sentiment (Nielsen, 2011) and cluster analysis (Lin, 2007) software tools. A first analysis of the 936 items revealed four main stakeholders: (1) citizens, including private bloggers; (2) Danish Government officials; (3) Business representatives; and (4) Professionals. A classification of analysis the 936 items revealed four types: (a) 204 letters to the editor (LttE) from citizens, (b) 91 articles from academic experts and professionals, and (c) 641 articles by journalists. A sentiment analysis (Nielsen, 2011) on the 934 items enabled us to identify two interest groups (IG): (IG1) citizens, bloggers and civic organizations, and (IG2) private sector professionals and government officials. This analysis also showed increasingly more negative sentiment from IG1 than IG2 over the period of the study. We then conducted a cluster analysis identifying 10 repeating themes (cf. Appendix A). Finally, using principles of critical hermeneutics (Ngwenyama and Lee, 1997) we read each item within a cluster to interpret its semantic meaning in context (cf. Appendix C for illustrations). From this analysis we summarize three dominant risk themes from the discourse which we present in the next section. ***Theoretical redescription***: To develop our *theory of the problem*, we use a critical interpretive strategy to analyze the empirical observations from the CDA, to derive and theoretically elaborate a set of conceptual categories and their relationships (Blaikie, 2007; Ngwenyama and Klein, 2018). Building on our understanding of the specific perspectives of the three stakeholder groups, we used an abductive strategy to theorize the empirical observations of the three risk themes. This required, going back and forth between empirical observations and literature to identify and elaborate core conceptual categories emerging from the discourse. We then used a retroductive strategy (Ngwenyama and Klein, 2018) to surface and test the *situational-logic* of the problem space in order to build the most plausible theoretical explanation of it. We used the qualitative technique of causal loop modelling (Yearworth & White, 2013) to model the relationships and interaction dynamics among the conceptual categories (cf. Figure 1). The findings from this theoretical redescription are reported in the Theoretical Discussion section of the paper.

>> Insert Table 1 about here

Background and Public Discourse

Digital Risks and the NemID

In 1994, the EU Parliament released the *Bangeman* report on digitalization, and the Danish Government announced its national digitalization strategy which included a personal digital identifier (eID) for Danish citizens. In 1999, the European Parliament issued directive (1999/93/EC) obliging member-states to implement an 'electronic signature' for its citizens, with the objective to "enhance trust in electronic transactions in the internal market". In 1994, when the idea of eID was introduced, the Internet and digital services were embryonic stage and the eID was not mandatory for Danish citizens. As per the 1999 EU directive, the Danish Government passed a law on electronic signatures in 2001 and introduced the first generation eID in 2003. Between 2001 and 2016, the Danish Government embarked on massive technology modernization to transform the country into a digital society. In 2009, 83% of adult Danes had home Internet access and 66% used home-banking (Statistics Denmark, 2010). In the same year, the government announced second generation eID, called NemID and made it mandatory for all Danes by July, 2010. The NemID infrastructure is now necessary for home-banking and access to all Danish government services (Henriksen, 2015; Madsen & Kræmmergaard, 2015). Consequently, reliability of and public confidence in the NemID infrastructure are essential to citizens whose everyday lives depend on it (Madsen & Kræmmergaard, 2015; Berger, 2015). As stated earlier, we are interested in how public officials in Denmark used the public sphere in responding to digital risk events causing fear and uncertainties among the citizens. In the following, we present a summary analysis of the three important digital risk events that dominated the public discourse.

Usability of the System

In July 2010, the NemID, was launched. An official website announced to the public that "NemID is safe, reliable and easy to use; no special software installation is required" (nemid.nu). The novelty compared to its predecessor was that "it is accessible from any computer over the internet as long as the user remembers their user-id and password and uses their physical keycard with 148 unique keys" (nemid.nu). On launch day, the Minister of Science and Technology, Mrs. Charlotte Sahl Madsen proclaimed, '*NemID is a quantum-leap forward', and 'a unique opportunity to get citizens to move to digital channels, which is only possible if it is* '*safe and easy to use*" [JP 02.07.2010]. The Minister then assured the public that the two-factor NemID authentication was safe and easy to use *as she had herself tested it*. On July 2, 2010 the newspaper Berlingske reported the following statement by Mrs. Charlotte Sahl-Madsen, Minister of Science and Technology:

> *"Digitalisation's version of the Great Belt Bridge." … "It is both more secure and easier. It opens up a whole universe with one entry point and one user ID," [BER 02.07.2010].*

Citizens, however, found the two-step authentication login procedure challenging to use. It required the user to enter a personal ID number and password of their own choice; then a Java applet generates a number,

which has to be matched with a 6-digit code from a card with 148 codes. In particular, elderly people found it too complicated. Media coverage focused intensely on the challenges of using the NemID. A heated discourse on the usability of NemID erupted in the press, with citizens and interest groups joining the debate.

The public discourse was further invigorated when Members of the parliamentary committee also rejected the *'safe and easy to use'* NemID. Professional spokespersons and critics raised concerns about the risk of marginalization of elderly and less educated populations. Professional and semi-professional spokespersons along with public opinion makers contributed with longer feature articles where they aired their indignation over the hostile digital society. The public debate on the usability of NemID continued for many months. In the first six weeks of NemID, Danes grew increasingly anxious about their futures in the emerging digital society. Four months after the launch, a citizen aired deep frustration in a letter to the editor of Jyllands-Posten:

> *"I was struggling on Sunday night to connect to my online bank. I was rejected without explanation. I was asked to contact NemID where an automatic answering system informed me that it was outside opening hours. The NemID web site did not mention anything about problems" [JP 04.11.2010].*

The discourse reflects dissatisfaction and frustration from end-users but also assurance from both public and private stakeholders who are promoting the NemID; it reflects a verbal battle over usability and design. The Minister in charge found the criticisms trifle and stated:

> *"It is predictable that such a large project becomes subject to discussion and critique, because everybody wants to comment on even the smallest grain of sand in the machinery"* [BT 16.09.2010]

Many citizens did not find the system to be either innovative or easy to use. Many had difficulties comprehending the specific requirements needed to use the system, as illustrated by the following:

> *"Look at this: Win 98, Win 2000, Win ME, XP, Mac-OS, Linux, Android, Vista, Win 7, 32 bit, 64 bit. What does that mean to the ordinary citizen? When using NemID you have to keep your operating systems and IE 8, Safari, Opera, Firefox etc. updated" [Letter to the editor JP 25.09.2010]*

The usability problems escalated soon after the launch; the NemID infrastructure experienced its first risk event that sparked "fear and anxiety of anticipated catastrophes from the new technology" (Beck U. , 1992b; Beck U. , 2009) was aired. As the empirical evidence shows, many Danish citizens were deeply anxious about managing their affairs online using the NemID infrastructure for fears of being locked out of banking and other vital transactions. However, citizens' rejection of the NemID was not an option as it would impede the digital society modernization project and reflect badly on the government and, in particular, on the Minister in charge of the modernization project.

Security Breaches of the System

On the day of the launch of NemID, concerns about the vulnerability of the infrastructure arose. To pacify the concerns, Johnny Bennedsen, the director of Nets and owner of the NemID infrastructure, stated:

> *"You can feel very safe using this solution. Our first priority is safety, safety and safety. We have done everything possible to make sure that the system works properly," [POL 02.07.2010]*

This attitude was shared by the minister in charge, the Consumer Protection Association and the Danish Bankers' Associations. However, the news media challenged it. For example, Politiken, ran article for consecutive days: "The new digital signature makes Denmark vulnerable" [POL 02.07.2010], and "New NemID is a temptation for hackers" [POL 03.07.2010]. In these articles, experts and researchers discussed the risks of a single entry-point to this critical information infrastructure. They argued that the risk exposure is too great for the nation 'when all eggs are put in one basket'. The head of the National Danish Police concurred, stating: "It would be a surprise if criminals do not try to challenge that system" [POL 03.07.2010]. A prominent professor joined the debate stating: "This is the first time in history where we have a single point for the national financial transactions. That is an attractive target. A single stroke can paralyze the economy" [POL 03.07.2010].

On August 9, 2010, 1 month after the launch of NemID infrastructure the first breached was reported. A day earlier, a Danish consumer protection spokesperson had claimed, *"We are positive about NemID. It is more secure than the previous system. So it is fundamentally good for consumers"* [EB8.08.2010]. When it was leaked that Nets withheld information on the infrastructure vulnerability, they admitted they to fix it when the attack occured. They stated: "*We should probably have warned the users about the Nemid.dk domain…. We will do that now*" [POL 14.09.2010]. A public official explains the suppression as follows: "*We had a justified expectation that we could have stopped it earlier, but we were unsuccessful*" [POL 14.09.2010]. On September 10, 2010, in parliament Folkparty IT spokesperson, Hanne Agersnap, in questioning Minister Charlotte Sahl-Madsen is reported to say: "*It seems that the authorities are afraid of the public and would rather try to keep a security breach secret…*" [POL 15.09.2010]. Responding a few days later, Minister Charlotte Sahl-Madsen said:

> *"It is expected that such a massive project is subject to debate and criticism, because everybody wants to comment on the smallest grains of dust in the machine. However, I still have great confidence in the NemID. I am convinced of the great significance of NemID for the digitization of the nation" [BT 16.09.2010].*

As fear erupted following the first breach, a concerned citizen stated: "*I haven't heard anything about citizens not being sufficiently protected. But wouldn't it be better to find ways to prevent [identity] theft?*" [JP 21.06.11]. The Central Personal Registry number (CPR), used in the NemID login procedure is also the primary key of all government data on Danes health, finance and social status; consequently, data breaches were a serious

concern and a recurring theme of the discourse. Reports of risk events intensified the fears Berlingske reports:

> *"Attempts to steal directly from Danes' bank accounts are now just as intense as they were before NemID was introduced. The number of break-ins in online banks is now back to its 2008-level. But Nets, who is responsible for NemID, is leaving it to individual banks to tighten their security" [BER 13.02.2013].*

On March, 12, 2013, a distributed denial of service (DDoS) attack made the NemID infrastructure inoperative for 3 days. A few days another attack was reported: "NemID closed down again" [BER 17.04.2013; BT 17.04.2013]. Citizens trust in NemID was further eroded when a group of teenagers, the LulzTeam, tweeted they had attacked the NemID to expose its vulnerabilities [BER 12.04.2013]. A Nets spokesperson, Søren Winge admitted that NemID was vulnerable to these types of attacks, but tries to down play the potential harm:

> *"We are constantly trying to find better ways to protect the infrastructure – but we have to admit, that it is probably not the last time we experience such attacks……It happens that we experience that we get thousands of requests for the eID, this results in system break-down. The requests result in traffic-jam in the system.... It is not hacking where someone tries to get your money or other sensitive data" [BT 12.04.2013].*

The news media were extremely critical of Nets and the public officials, and keen to highlight the silence of Danish Emergency Management Agency (DEMA) on the issue. Experts also recognized the security challenges facing the Danish digital society. For example, the IT-security expert Peter Kruse points out:

> *"The police have a very bad case, when trying to find those responsible for the serious attack today…..Hackers are not so stupid that they use their own IP-address, when they attack the system. Therefore, it is almost impossible to find them". [POL 12.04.2013]*

These short excerpts from the discourse illustrate the helplessness citizens felt on being forced to adopt the NemID. This strand of the debate continued for nine months after the launch of the NemID, with the newspaper Jyllands-Posten dedicating a section to the topic [JP 21.06.11]. In total 136 journalistic articles were published with experts challenging the security and encryption vulnerabilities of the NemID infrastructure. Citizens wrote 25 letters to editors about concerns of identity theft and cybercrime from using NemID. A first and noteworthy article on identity theft was published by a blogger, Dorte Toft. She called for an ombudsman to be instituted, stating: "*The person who gets their identity and/ or money stolen can end in a Kafkaesque nightmare*" [BER 09.09.10]. She also argued that, unlike physical goods, no one cares about the theft of digital assets, and the burden of proof is entirely on the victim, who can easily get lost in the digital universe.

Sale of the NemID Infrastructure

A third event to escalate the citizens' perception of risk was the announcement that Nets wanted to sell the NemID infrastructure. Nets was owned by Danish and Norwegian banks, with the Danish National Bank owning 10% of its shares. On June 18, 2013, the Danish business daily Børsen reported that Nets was seeking a buyer and hired the US firm J.P. Morgan to manage the sale. The Børsen article stated; *"The owners feel that the*

time is right to sell Nets and the process has been started." A new theme had entered the ongoing public debate on the NemID and risks to Danish society. Eighty articles and expert commentaries appeared in the media raising fears that the NemID infrastructure could be sold to Chinese investors. A core concern of the experts also revolved around the absence of robust international law to support individual data-protection. The US and EU regulations on data-protection differ and it was not clear which set of rules would apply to the new American owners. The Snowden revelations of US National Security Agency's surveillance on foreign nationals (including heads of states) only served to intensify these concerns. This triggered a heated discourse among citizens, politicians, and other key stakeholders. The prospect of foreign nations getting access to private data created much anxiety among citizens and commentators. There was also widespread concern about the general behavior of investment firms whose strategy is to increase prices, and optimize earnings by stripping off healthy parts of businesses and selling them at a profit to interested investors. On June 19, 2013, Berlingske reported on a parliamentary debate Hans Kristian Skibby of Danish People's Party raised concerns about the implications of foreign ownership of NemID, and proposed to nationalize Nets:

> *"Our central payment system must definitely not get into the hands of a Chinese or American capital fund. I would propose that the government buys Nets if the Americans, Chinese or others try to meddle in our payment systems," [BER 19.06.2013].*

The Red-Green Alliance also supported the nationalization of Nets, which prompted the following response by the Business and Growth Minister, Minister Annette Vilhelmsen:

> *"A potential new owner must not abuse its position, for example by raising prices. This is something we will follow very closely. If there are new investors in Nets, I would expect them to be aware that the government places a great deal of emphasis on a well-functioning market for payment systems," [BER 19.06.2013].*

Citizens again contributed to the debate with 16 letters to the editors expressing their fears of the potential loss of control of information privacy that could accrue from foreign ownership. The following comment in a letter to the editor of Berlingske characterizes the general feelings of Danes:

> *"Now they are talking about the banks selling PBS, with NemID and everything! What security do Danes/users have that the buyers don't use the goldmine of personal information they are buying in undesirable ways? Where are we going?" [EB 20.06.2013].*

The debate over the control of the NemID infrastructure intensified and took on an ideological tone. The idea of selling Nets to foreign owners brought back memories of the ethical dilemma that Danes had faced a few years earlier when the state-controlled Dong Energy was sold to the U.S. investment bank and hedge fund Goldman Sachs. Danes viewed Goldman Sachs' role in the 2008 collapse of financial markets very negatively and questioned how their politicians could allow vital energy infrastructure to be sold to 'financial vultures'. Experts were keen to point out that both NemID and the mobile phone network are components of critical national infrastructure upon which society depends. Danish society would be exposed to considerable risk if

foreign companies were allowed to control national infrastructure. Citizens agreed with the experts. In letters to the editor of Jyllands-Posten, two citizens stated:

> *"The country's IT infrastructure is much too important to allow important parts of it to be owned and operated by foreign companies," [JP 10.12.2013].*
> *"Nets controls the state-required NemID, so our personal data goes into the pockets of a foreign company, without any possibility of opting out. Yes, the world is global and competition is international, but it's not forbidden to think twice before the bank directors simply sell to the highest bidding capital fund," [JP 03.01.2014].*

On the issue of the sale of Nets to foreign owners, however, government and business were in alignment. Some Danish business executives argued that foreign investment was necessary for the continued modernization of the NemID infrastructure. Peter Lybecker, Chairman of the Board of Nets, claimed the company needed new owners having *"the necessary expertise and financial strength to bear the very large IT investments that are necessary to survive and develop in an increasingly international and competitive market"* [JP 31.12.2013]. In February 2014, the Minister of Business and Growth, Mr. Henrik Sass-Larsen supported the sale of Nets. In press conferences, he stated that 'there is no reason for concern about the sale of Nets' [BER 09.02.2014]. He is also reported as making the following statements:

> *"Neither the Consumer Protection Agency nor the Confederation of Danish Enterprise see any problem with the sale. The Confederation finds it exciting to see the dynamism that a new owner can bring to Nets," [JP 08.02.2014].*
> *"The regulations and agreements that apply today to Dankort, Payment Service and NemID will not change in case the company is sold.....Nets will continue to be under the control of the Financial Supervisory Authority,*" [BER 09.02.2014]

While many of the journalistic articles discussing the possible sale of Nets focused on how hedge funds function, they were keen to mention the potential windfall profit to Nets, as well as ethical concerns about personal data on Danes falling into foreign control. On February 13, 2014 newspapers reported that bids were in for the sale of Nets. The debate intensified around information privacy issues, and which foreign equity fund could be an appropriate owner for Nets. Hans Christian Skibby (DF) stated: *"It makes a difference whether counterpart on the other side of the table is Danish or an American or Chinese private equity fund,"* [BER 19.06.2013]. The opposition politician Michael Aastrup Jensen argued: "*there is a great deal of reason for concern about security, if we move Nets data outside of Denmark,*" [BER 13.02.2014]. Minister of Business and Growth, Mr. Henrik Sass Larsen admitted that he could not that guarantee the American government would not demand sensitive information from Nets, if it was owned by an American company. However, he was convinced that, "*There is no reason to believe that the Americans will demand the sensitive information,"* [BER 09.02.2014]. But Michael Budolfsen, vice chairman of bank employees in Finansforbundet, disagreed, stating:

> *"There will be a whole other legal regime, if Nets is bought by a buyer from a country far away, for example the United States*," [BER 13.02.2014].

On March 13, 2014, there was a parliamentary hearing on the sale of Nets. The issue was raised that two of the five bids for Nets were from American hedge funds. News of Snowden's leaks that the US National Security Agency was conducting surveillance on foreign nationals terrified politicians and Danish citizens. In the parliament, concerns were raised that the US Patriot Act enables the American government to demand information from American companies beyond what is acceptable under Danish and EU law. For many days, the vociferous parliamentary debates continued but there would be no nationalization. On March 24th, 2014, Peter Lybecker, chairman of Nets Holdings, announced the decision to sell off the company responsible for NemID infrastructure to a consortium of two U.S. investment firms, Advent International Corp. and Bain Capital LLC, and the Danish pension fund ATP for 17 billion Danish kroner ($3.14 billion). Lybecker states:

> *"The outcome of this review was that Nets needs a new owner with the expertise, commitment and financial resources to develop the business in a rapidly changing payments industry.....I strongly believe that we have found a highly-qualified owner of Nets in the consortium consisting of Advent International, ATP and Bain Capital, which has the right balance of strong local roots and considerable global expertise within the payment systems sector.....,"* [BER 25.03.2014].

The debate on ownership revealed extensive, broad-based concerns about the risks to information security arising from foreign control of Nets, the company responsible for the NemID infrastructure. Meanwhile, the Nets management was keen to reassure the public that security had a high priority with the buyers, while the investment firm managers pointed out that the Danish pension fund ATP which was minority owner has a veto over exchange of data between Denmark and US. However, as a journalist pointed out; *"It is most unlikely that the NSA would ask ATP for permission before going on a data-hunt"*. The Minister of Justice, Mrs. Karen Hækkerup, found it unrealistic to expect that the Danish Data Agency would be capable of uncovering data security breaches of the type described by Snowden [BER 25.03.2014]. Responding to the Danes' concerns, Robin Marshall, managing partner at Bain Capital was reported to have said: *"Data security has the highest priority for us in the coming years,"* [POL 25.03.2014]. While Danish citizens can feel a limited sense of control over their own government and companies that operate under Danish law, the sale of Nets raised the question of whether operation of the NemID infrastructure and control of the data passing through it would be protected by Danish and European law.

Theoretical Discussion of Findings

In this research we set out to develop an understanding of the risk communication challenges facing public officials in the emerging digital risk society. In the prior section we presented a descriptive analysis of the public discourse that revealed three dominant risk themes and interactions among key stakeholders. In this section we focus on theoretically elaborating four categories of issues in the problem space derived from our analysis of the discourse. As Luhmann (2002, pp.41) argues, in the temporal flux of risk discourse a core phenomenon of interest are the categories of issues that shape our societal problems (see also Fischhoff,

1995). Figure 1 presents a theoretical redescription of the problem space using a causal loop model to represent the interaction dynamics of four core categories: (1) Ideologies of Modernization; (2) Escalating Fear; (3) Distorted Communication; and (4) Institutional Credibility. This model maps the core dimensions of the public management risk communication challenge we observed. Figure 1 illustrates a complex set of positive and negative influences and reinforcing dynamics: At the general level, *Ideologies of modernization* played a generative role in the problem space motivating digital proliferation and adoption, which precipitate expanding digital risk events. Expanding digital risk events and *distorted communication* about them undermine public trust in *institutional capabilities* influences *fear escalation*. These observed dynamics resemble those explicated by Beck (1992a&b, 2015) with one fundamental difference: the risks are not environmental and arising from industrialization; they are social, arising from invasive digitalization of society, with profound consequences for the social cohesion and the legitimacy of social institutions. In this regard, a theoretical discussion of these four categories is essential to foundational research for developing solutions to the problem. In the following we discuss each category linking it to relevant theoretical discourses in order to develop a broad understanding of the core issues of the problem space.

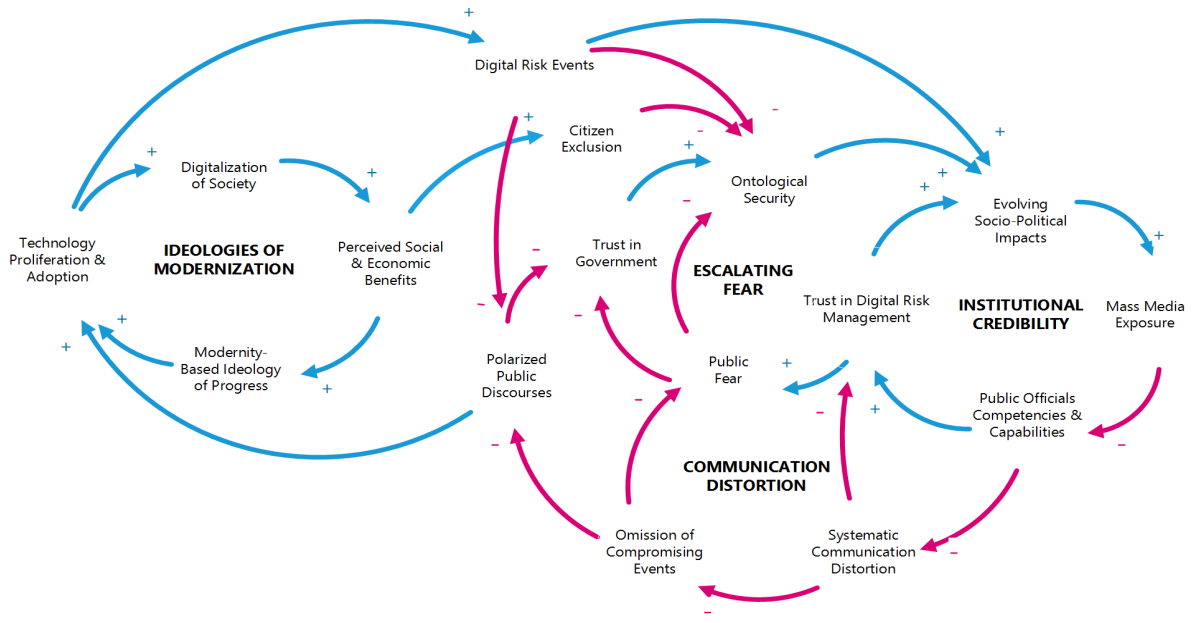

Figure 1: The Interlocking Dynamics of the Digital Risk Society and Public Management Challenges

Ideologies of Modernization

While the Danish media played a role in shaping narratives of modernization, the key propagandists of *ideologies of modernization* in the context of the NemID project were government officials and business

stakeholders. These ideologies drove decision making in this public-private partnership project, and were repeatedly used for symbolic value in *distorted communication* and rational appeals to assuage citizens when fear and anger escalated over the seemingly uncontrollable digital risk exposures. Elsewhere, researchers observe that *ideologies of modernization* drive governments to collaborate with business enterprises on ever more invasive forms of societal digitalization that expose citizens to social risks (Rowe, Ngwenyama & Richet, 2020; Sundberg, 2019; Lyon, 2017). Ideologies of modernization are a critical factor in the rapid digitalization of society. Researchers have noted that governments now follow 'digital by default' strategies, the approval and roll-out of digital infrastructure without clear understanding of social risks (Corydon, Ganesan & Lundqvist; 2016; Rowe, et. al., 2020). Digital technology is viewed as a magical force capable of transforming all social forms-of-life, civilizing and making us more human (Stahl, 1995; Adas, 2015; Curran, 2018). Societal digitalization is now seen as critical for expanding democratic rights (Nam, 2017), wealth accumulation and economic prosperity (Asongu & Odhiambo, 2020; Hornborg, 2014), and advanced nation state status (Katz & Koutroumpis, 2013). In the absence of critical social analysis, these beliefs constitute a powerful ideology that drive governments to collaborate with business actors to aggressively push digitalization of society, excluding citizens from decision making processes and undermining government regulation (Beck, 2006; Zuboff, 2019). Denmark adopted the modernization discourse without reservations. As illustrated in the previous section, it aggressively pushed the NemID infrastructure project (cf. Appendix B for key events), using these ideological arguments to justify decisions in the face of escalating risks and citizen resistance (Igari, 2014). The ideology of digitalization is now a global phenomenon, its central tenet is it will improve the quality of life of citizens and bring social and economic benefits, so we must accept the risks and uncertainties that accrue from it (Brynjolfsson & McAfee, 2014; Caruso, 2018). Governments push digitalization of public services and corporate actors embed digital systems in every possible product and service. Citizens are excluded from decision making on the digitalization of their everyday lives. There is no mechanism for participatory decision making concerning the digital world we are building, citizens are simple subjects of the decisions and plans of governments and private companies but must accept the emerging risks exposure (Miranda, Young, & Yetgin, 2016; Zuboff, 2019).

Escalating Fear and Digital Risks

Our empirical observations from the public discourse on NemID showed that unpredictability of social risks from digitalization was a fundamental issue for Danish citizens. Expanding digital risk events and the *distorted communication* about the risk exposure by government and company officials undermined the public trust and contributed to the *escalation of fear* among Danish citizens. The media amplified the citizens perception of the risks with increasing number of stories and scenarios of digital risks and their potential consequences. In turn, citizens responded with letters-to-editors expressing their fears and anxiety about potential harm from the frequent attacks on the NemID infrastructure. While these dynamics typify our case study, they also

represent a more general pattern of a category of social problems arising in the new digital risk society (Knight and Saxby, 2014; Curran, 2018; Elhai, Levine and Hall, 2017). Aggressive societal digitalization is spawning new social digital risks phenomena that are affecting citizens and society: (1) digital surveillance for profit and political control; (2) denial of service attacks to financial and banking infrastructure; (3) data breaches, identity theft, ransom and extortion; (4) hacking and cyberattacks on national infrastructures; (5) manipulation of democratic elections. When such risk events occur, they engender fear and helplessness in public officials and citizens alike (Galbraith, 2012; Knight & Saxby, 2014). Digital technologies are unpredictable and unruly, government officials and corporate actors cannot anticipate the scale or complexity of their risks to society. In our case study, the Danish government could not have envisioned the digital risk events that would challenge institutional capabilities for managing state and citizen security. Danish citizens too could not have predicted that a seemly simple digital artifact, the NemID, would set in motion a process of escalating risks that would threaten their sense of existential security and access to fundamental services. The continued escalation of risk events rapidly also exposed the limitations of social institutions (administrative and scientific) for predicting, recognizing, managing the digital risk society. However, as Beck (1992a &b) points out, this is the fundamental contradiction of the risk society; it is of our own making, resulting from the commitments of governments and business interests to exploit modern technologies for social and economic benefits for the continued 'progress' of advanced societies.

Recent research has shown that digital risk events of large-scale data breaches, denial of service attacks and identify theft can lead to spiraling fear and moral panic of citizens (Mirea, Wang, & Jung, 2019; Hier, 2019). Digitally unsophisticated citizens and especially senior citizens, who are increasingly targets, fear that identity thieves could drain their bank accounts and cause them financial ruin (Walsh, Shiu, Hassan, Hille, & Takahashi, 2019). In our case study, another factor that stokes fear was who would 'own and control' the data in the NemID infrastructure; a significant concern, growing larger in this era data capitalism and limited regulation on data capitalists (Wright & Xie, 2019). The practices of data capitalists of acquiring data from varied sources and 'quilting' them together is generating extreme risk exposure to citizens when there are data breaches (Anandarahan & Hill, 2019). Those who suffer the harm are responsible for repairing it, while the data capitalists are required to do no more than notify them that their data has been breached (Clarke, 2019; Zuboff, 2019). A third factor stoking citizens' fear is press reports of data breaches (Chatterjee, Gao, Sarkar, & Uzmanoglu, 2019). In our case there were a large number of media articles discussing, not only the specific risk events, but global events of hacking, information warfare, identity theft and loss of digital assets. This too is a defining characteristic of the digital risk society, in which news media and Internet stories amplify fears and anxiety of citizens (Chung, 2011).

Institutional Credibility

In our case study we also observed that *escalating fear* and *distorted communication* of public officials

undermined the Danish citizens' reflexive trust in their societal institutions. Similar institutional dynamics have been observed by other researchers who examined a variety of societal risk situations (cf. Beck, 2006; Luhmann, 2005; Grönlund & Setälä 2012). In letters-to-editors, Danish citizens increasingly questioned the capabilities of government officials and company executives to manage the escalating risk events on the NemID infrastructure. When the digital risk events escalated, Danish government officials could give no credible responses, and seem to depend on academic experts to explain the intricacies of the situation. Another of the citizens' concern was which jurisdiction would have legal oversight of their data after the sale of the infrastructure. Again, government officials could give the citizens no satisfactory responses; the new foreign owners of the infrastructure were not under the jurisdiction of Danish law. As news reports increased on scale and impact of data breaches continued to emerge, fear escalated and the citizens' trust in government institutions eroded. Our empirical observations of the eroding confidence in government institutions and reputations of the company executives is supported by recent research (Curran, 2018; Chatterjee, Gao, Sarkar, & Uzmanoglu, 2019). Elsewhere, researchers found that individuals blame the companies for not exercising duty of care with their data and government regulators for lax laws that encourage lax data management practices in the companies (Allen & Peloza, 2015; Carre, Curtis, & Jones, 2018). Furthermore, research have also found that lax enforcement of data regulations and lack of financial penalties for violations, encourage companies to ignore their responsibilities in protecting the data of individuals the hold in their systems (Hemphill & Longstreet, 2016; Park, 2019). The continuing reports of data breaches and the vastness of their impact not only stoke fear in citizens, but trigger anger and resentment at companies whose systems are breached and governments for not enacting regulations and enforce compliance (Allen & Peloza, 2015; Sloan & Warner, 2019).

Distorted Communication

The digital risk events that unfolded during the implementation NemID infrastructure presented Danish public officials and company executives communication dilemmas. For public officials, digital risk communication posed a dilemma of divided loyalties: push digitalization at any cost, or proceed with caution to minimize risks to citizens. However, in spite of expanding digital risk exposure, the Danish public officials chose to show uncompromising commitment to the digitalization project, even when experts criticized its robustness. They responded using systematically distorted communication, misinformation, abstract technical language, and ideology (of modernization) as a strategy of 'impression management' (Allen & Caillouet, 1994; Jenkins, Anandarajan, & D'Ovidio, 2014). Rather than acknowledge the seriousness of the issues, both company and public officials responded with *false* narratives about the safety and reliability of NemID infrastructure, in the hope of convincing the citizens the risks were 'not high, but expected'. The officials falsely downplayed the security risks to citizens' personal data, and more importantly violated Danes expectation of open communication. The infrastructure owner gave repeated assurances of its robustness, while trying to shift the

discourse to its importance for social and economic growth. Danes expected transparency from their public officials, and government protection of their wellbeing; and these expectations were openly discussed in parliamentary debates. The use of systematically distorted communication by the Danish officials had a corrosive effect on their credibility. The citizens openly questioned their credibility and competence, as well their government's capacity to protect their interest. Recent research support this finding that public official's use of distorted communication can damage the credibility of government institutions (Gross, 2010; Kalgin, 2016). Some studies also directly link decreasing confidence in government institutions with the behavior of public officials (Grönlund, 2012). When public officials systematically make false statements about critical issues, trust is eroded and the capability to mobilize public support for critical projects diminished (Gross, 2010; Seyd, 2015).

Another issue to which Danish officials responded to with systematically distorted communication was the citizens' outcry over the potential sale of the infrastructure to a private entity outside the EU. When the owner Nets announced it was searching for a buyer, citizens voiced their fears at losing control of the infrastructure and their information assets. They questioned how the company is allowed to sell *'their data'* to someone else; they believed it to be public infrastructure. It was extremely difficult for Danes to comprehend its sale, when they paid for with their taxes. When they protested its sale to a foreign buyer, not to subject Danish or European data protection laws, the public officials and company executives remained silent. While EU law protected individual data security, no such protection existed in international law. Nets chairman, Lybecker simply stated the company needed investment and expertise, and that the new owners 'would be highly dependable'. This was distorted communication (*falsehoods*); first the infrastructure was already paid for by tax payers; second there was no possibility to know what the new owners would do. Profit maximization logic dictated its sale, the NemID infrastructure had no competitors, and its use was mandated for all Danish citizens. The government insisted that all Danes 'must' use it for all financial transactions, and invoked free market logic to explain why they could not stop the sale. This was a new revelation that the government (Danish citizens) owned neither their data nor the NemID infrastructure. It was built by a typical public private partnership (PPP) between the government, who mitigates the risk and the private partner who maximizes return (Takashima, Yagi, & Takamori, 2010). The terms of the PPP contract were withheld from the public until the issue of the infrastructure sale emerged. Not surprisingly, the disclosure further eroded trust in the officials and undermined the credibility of the government. These and other incidents illustrate the communication dilemmas of public managers in the digital risk society; as risk escalates, public officials are forced to respond with: (a) incomplete and inaccurate information, (b) to unanticipated outcomes of prior decisions, and (c) sometimes must take untenable positions. The use of systematically distorted and strategic communication in such situations can damage reputations of officials and trust in public institutions (Keohane, 1998; Seyd, 2015;

Rowe, Ngwenyama & Richet, 2020).

Conclusion and Limitations

In this paper, we set out to develop a *theory of the problem* of public management communication about digital risk events which have the potential to instill fear and erode trust in societal institutions. Using Beck's concept of the world risk society (Beck 1992a, 2006), and concepts from Habermas's (1991; 2006) theory of communicative action we interrogate public discourse concerning the NemID infrastructure deployment and digital risk events to develop a theoretical understanding of the emerging social dynamics of *digital risk society*. We are not claiming that our theory outlined above and illustrated in Figure 1 is a complete definition of the problem space. As Majchrzak, Markus, & Wareham (2016) point out there is rarely "a *single clear consensus problem statement on a substantive [IS] problem and agreement on causes, and contributing factors, let alone on if or how the problem should be solved*". What we do claim is that our theory is a substantive definition of the problem space which offers some insights to advance research and knowledge development for improving digital risk management of the digital risk society. Presently, there is little published research in this critical area at a time when social risks from societal digitalization are expanding (Gimpel & Schmied, 2019). A general theory of the problem is an important first step in devising a theory of solution strategies for this new and emerging area of critical concern. As our findings illustrate the digital risks were invisible, not anticipatable, uncontrollable and frightening to ordinary citizens, characteristics of the digital risk society. When risk events occur, government officials face dilemmas of action based on inadequate knowledge of these complex problems. A poignant example is the July 19, 2019 decision of the Louisiana state governor to declare a state of emergency after a set 'severe breaches' of the public digital infrastructure (Mathews, 2019). In pursuing digitalization for social and economic progress, public officials face emerging challenges to state security and the wellbeing of citizens from escalating digital risks (Gross, 2015). They must often: (a) champion digital infrastructure of unknown, unanticipatable and incalculable risks to society; (b) collaborate with private companies whose principal interest is in maximizing personal profits and not the commonwealth; and (c) oversee digital innovations of which they have limited knowledge. Ideologies of modernization have a powerful influence in how government elites envision social and economic progress. The scope and reach of digitalization everyday private and public human activity have given rise to the concept of the digital citizen (de Moraes & de Andrade, 2015). In new digital risk society, every activity of the digital citizen is subject to surveillance, and these data are collected, aggregated, curated and resold by data traders of questionable ethics, whose singular interest is in profit maximization (Zamora, 2019; Lyon, 2017).

We lack capabilities for managing the societal risks of emerging digitalization and the exponential rise in digital risk events, whose scale, complexity, global reach and impact on the daily lives of citizens and our institutions are incalculable (Gross, 2015). Government officials and public management experts who must develop policies, legislation and strategies for defending the rights of citizens and mitigating the harm of digital risks

events to citizens and societal institutions are overwhelmed by the challenges (Albahar, 2017; Sloan & Warner, 2019). As social scientists concerned with IS phenomena we have both opportunity and responsibility to develop knowledge for addressing these issues (Schultze, 2017; Ngwenyama & Klein, 2018). However, if we (IS researchers) are to contribute to solutions for more effective public management of the digital risk society we need to develop a *theory of the problem* (Majchrzak, Markus and Wareham, 2016). Our critical theoretic approach enabled the systematic interrogation of some important issues in the dynamics of the digital risk society. Specifically, the emergent challenges of digital risk events and their implications for the public management of democratic societies. Our empirical research offers new insights into the social and political dynamics of the digital risk society.

The theory of the problem outlined in this paper provides a broad theoretical description of the problem space of public management risk communication challenges upon which a substantive research program can be built for advancing knowledge about the digital risk society. While there is a small emerging body of work (Rowe, Ngwenyama & Richet, 2020; Schultze, 2017; Whitley & Hosein, 2008), much more research is urgently needed. As societal digitalization intensifies and most IS research remains focused on 'economic interest' and generating 'business value', the knowledge deficit is rapidly widening. For example, our theory could assist in much needed research to develop effective digital risk communication strategies to address citizens' fear and anxiety when crises emerge (Hiers, 2019). While there is much research on public health and natural disaster risk communication (cf. Lundgren & McMakin, 2018), there is hardly any literature on digital risk communication. Second, it can offer insights to guide research to facilitate citizen engagement in decision making about public digital infrastructure. Such involvement can also help reinforce institutional credibility and trust in government officials in times of crisis. Recent studies have shown that countries with more open and collaborative decision-making practices on digital infrastructure fared better with deployment and use of COVID-19 apps (Rowe, Ngwenyama & Richet, 2020). A third finding of this research that could benefit from further research is the value conflicts between ideologies of digitalization and democratic values. Decades ago IS researchers warned about the potential value conflicts of mass digitalization (Kling, 1978; Klein, 1981), however, the race to societal digitalization for economic returns and 'digital first solutionist' ideologies (Morozov, 2013; Baskerville *et al.*, 2020) have inhibited our understanding of the potential dangers. Every new technology brings with it new, poorly understood social risks and difficult to comprehend societal implications (Rasmussen, 2006; Beck, 1992b). In this regard, 'digital first solutionist' ideologies need to be reconsidered as they expose society to expanding risks from unregulated digital experiments by tech companies and governments.

References

ADAS M (2015) *Machines as the measure of men: Science, technology, and ideologies of Western dominance.* Cornell University Press.

ALBAHAR M (2017) Cyber attacks and terrorism: a twenty-first century conundrum. *Science and engineering ethics,* **25(4)**, 993-1006.
ALLEN AM and PELOZA J (2015) Someone to watch over me: The integration of privacy and corporate social responsibility. *Business Horizons,* **58(6)**, 635-642.
ALLEN MW and CAILLOUET RH (1994) Legitimation endeavors: Impression management strategies used by an organization in crisis. *Communications Monographs,* **61(1)**, 44-62.
ALTHEIDE, D. L. (2013). Media logic, social control, and fear. *Communication Theory,* 23(3), 223-238.
ANANDARAHAN M and HILL C (2019) Data quilting: Art and science of analyzing disparate data. *Cogent Business & Management,* ***6*****(1)**, 1-19.
ASONGU SA and ODHIAMBO NM (2020) Foreign direct investment, information technology and economic growth dynamics in Sub-Saharan Africa. *Telecommunications Policy,* **44(1)**, 1-14.
BASKERVILLE, R.L., MYERS, M.D. & YOO, Y. (2020). Digital First: The Ontological Reversal and New Challenges for Information Systems Research. *Management Information Systems Quarterly*, 44(2), 509–523.
BECK U (1992a) Risk society: Towards a new modernity (17). Sage.
BECK U (1992b) From industrial society to the risk society: Questions of survival, social structure and ecological enlightenment. *Theory, culture & society,* **9(1)**, 97-123.
BECK U (1997) Subpolitics: Ecology and the disintegration of insitutional power. *Organization & Environment,* **10(1)**, 52-65.
BECK U (2000) *Risk Society Revisited. Theory, Politics and Research.* (B. Adam, U. Beck, & J. van Loon, Red.)
BECK U (2006) Living in the world risk society: A Hobhouse Memorial Public Lecture given on Wednesday 15 February 2006 at the London School of Economics. *Economy and society,* **35(3)**, 329-345.
BECK U (2009) Critical theory of world risk society: a cosmopolitan vision. *Constellations*, **16(1)**, 3-22.
BECK, U. (2013). Why 'class' is too soft a category to capture the explosiveness of social inequality at the beginning of the twenty-first century. *The British Journal of Sociology,* 64(1), 63-74.
BECK U (2015) Emancipatory catastrophism: What does it mean to climate change and risk society? *Current Sociology*, **63(1)**, 75-88.
Berger JB (2015) E-government harm: An assessment of the Danish coercive digital post strategy. Roskilde: Roskilde Universitet.
BLAIKIE, N. (2007) Approaches to Social Enquiry: Advancing Knowledge, Polity Press, MA.
BROWN L and OSBORNE SP (2013) Risk and innovation: Towards a framework for risk governance in public services. *Public Management Review*, **15(2)**, 186-208.
BRUNK CG (2006) Public knowledge, public trust: understanding the 'knowledge deficit'. *Public Health Genomics,* **9(3)**, 178-183.
BRYNJOLFSSON E and MCAFEE A (2014) *The second machine age: Work, progress, and prosperity in a time of brilliant technologies.* WW Norton & Company.
CARRE JR, CURTIS SR AND JONES DN (2018) Ascribing responsibility for online security and data breaches. *Managerial Auditing Journal*, **33(4)**, 436-446.
CARUSO, L. (2018). Digital innovation and the fourth industrial revolution: epochal social changes? *AI & Society*, *33*(3), 379-392.
CECEZ-KECMANOVIC D, DAVISON RM, FERNANDEZ W, FINNEGAN P, PAN SL, SARKER S (2020) Advancing Qualitative IS Research Methodologies: Expanding Horizons and Seeking New Paths. *Journal of the Association for Information Systems* 21(1):246–263.
CHAKRAVARTTY P and SCHILLER D (2011) Global Financial Crisis| Neoliberal Newspeak and Digital Capitalism in Crisis. *International Journal of Communication,* ***4***, 670-692.
CHAN CM, HACKNEY R, PAN SL and CHOU T-C (2011) Managing e-Government system implementation: a resource enactment perspective. *European Journal of Information Systems,* **20(5)**, 529-541.
CHANDLER D (2019) Digital governance in the Anthropocene: The rise of the correlational machine. In Chandler D., and Fuchs, C. (Eds) *Digital Objects, Digital Subjects: Interdisciplinary Perspectives on Capitalism, Labour and Politics in the Age of Big Data*, University of Westminster Press, 23-42.
CHATTERJEE S, GAO X, SARKAR S and UZMANOGLU C (2019) Reacting to the scope of a data breach: The differential role of fear and anger. *Journal of Business Research,* ***101***, 183-193.

CHUNG IJ (2011) Social amplification of risk in the Internet environment. *Risk Analysis: An International Journal,* **31(12)**, 1883-1896.
CLARKE R (2019) Risks inherent in the digital surveillance economy: A research agenda. *Journal of Information Technology,* **34(1)**, 59-80.
CLEMENTSON DE (2020) Narrative persuasion, identification, attitudes, and trustworthiness in crisis communication. *Public Relations Review*, **46(2)**, 1-9.
COOMBS WT (2014) *Ongoing crisis communication: Planning, managing, and responding*. Sage Publications.
COOMBS WT and HOLLADAY SJ (2002) Helping crisis managers protect reputational assets: Initial tests of the situational crisis communication theory. *Management Communication Quarterly*, **16(2)**, 165-186.
CORYDON B, GANESAN V and LUNDQVIST M (2016) *Digital by default: A guide to transforming government*. New York: McKinsey & Company.
COTTLE, S. (1998). Ulrich Beck, Risk Society' and the Media: A Catastrophic View? *European Journal of Communication*, **13(1)**, 5-32.
CUKIER W, NGWENYAMA O, BAUER R and MIDDLETON C (2009) A critical analysis of media discourse on information technology: preliminary results of a proposed method for critical discourse analysis. *Information systems journal,* **19(2)**, 175-196.
CURRAN D (2018) Risk, innovation, and democracy in the digital economy. *European journal of social theory,* **21(2)**, 207-226.
DAHL A and SOSS J (2014) Neoliberalism for the common good? Public value governance and the downsizing of democracy. *Public Administration Review,* **74(4)**, 496-504.
DE MORAES JA and DE ANDRADE EB (2015) Who are the citizens of the digital citizenship. *International Review of Information Ethics,* **23(11)**, 4-19.
DUNWOODY, S. (1992). The media and public perceptions of risk: How journalists frame risk stories. In The social response to environmental risk (pp. 75-100). Springer, Dordrecht.
ELHAI, J.D., LEVINE, J.C. AND HALL, B.J. (2017), "Anxiety about electronic data hacking: Predictors and relations with digital privacy protection behavior", *Internet Research*, **27(3)**, 631-649.
FISCHHOFF, B. (1995). Risk perception and communication unplugged: twenty years of process 1. *Risk Analysis,* **15(2)**, 137-145.
GALBRAITH ML (2012) Identity crisis: Seeking a unified approach to plaintiff standing for data security breaches of sensitive personal information. *American University Law Review*, **62(5)**, 1365-1400.
GAMSON WA and MODIGLIANI A (1989) Media discourse and public opinion on nuclear power: A constructionist approach. *American Journal of Sociology,* **95(1)**, 1-37.
GERBER M and VON SOLMS R (2005) Management of risk in the information age. *Computers & security,* **24(1)**, 16-30.
GIL DE ZÚÑIGA H, VEENSTRA A, VRAGA E and SHAH D (2010) Digital democracy: Reimagining pathways to political participation. *Journal of Information Technology & politics,* **7(1)**, 36-51.
GIMPEL, H., & SCHMIED, F. (2019). Risks and side effects of digitalization: a multi-level taxonomy of the adverse effects of using digital technologies and media. *Proceedings of the 27th European Conference on Information Systems* (ECIS), Stockholm & Uppsala, Sweden, June 8-14, 2019. ISBN 978-1-7336325-0-8
GRÖNLUND, K. & SETÄLÄ M (2012). In honest officials we trust: Institutional confidence in Europe. *The American Review of Public Administration,* **42(5)**, 523-542.
GROSS AG (2010) Systematically distorted communication: An impediment to social and political change. *Informal Logic,* **30(4)**, 335-360.
GROSS O (2015) Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents. *Cornell International Law Journal,* **48**, 481-511.
HABERMAS J (1984) *The theory of communicative action.* Beacon Press.
HABERMAS J (1991) *The structural transformation of the public sphere: An inquiry into a category of bourgeois society.* MIT press.
HABERMAS J (2006) Political communication in media society: Does democracy still enjoy an epistemic dimension? The impact of normative theory on empirical research. *Communication theory,* **16(4)**, 411-426.

HEMPHILL TA and LONGSTREET P (2016) Financial data breaches in the US retail economy: Restoring confidence in information technology security standards. *Technology in Society, **44***, 30-38.
HENRIKSEN HZ (2015) *Scrutinizing open government data to understand patterns in egovernment uptake.* Springer, Cham.
HEPP A, ALPEN S, & SIMON P. (2020). Beyond empowerment, experimentation and reasoning: The public discourse around the Quantified Self movement. *Communications*, *1*(ahead-of-print). Published online: 24 Jul 2020. https://doi.org/10.1515/commun-2019-0189
HIER S (2019) Moral panics and digital-media logic: Notes on a changing research agenda. *Crime, Media, Culture,* **15(2)**, 379-388.
HORNBORG A (2014) Technology as fetish: Marx, Latour, and the cultural foundations of capitalism. *Theory, Culture & Society,* **31(4)**, 119-140.
HORNIG S., (1993) Reading risk: public response to print media accounts of technological risk. *Public Understanding of Science*. **2(2)**, 95-109.
IGARI N (2014) How to successfully promote ICT usage: A comparative analysis of Denmark and Japan. *Telematics and Informatics,* **31(1)**, 115-125.
INNES, A. J. (2010). When the threatened become the threat: The construction of asylum seekers in British media narratives. *International Relations,* **24(4)**, 456-477.
IRANI Z, ELLIMAN T and JACKSON P (2007) Electronic transformation of government in the UK: a research agenda. *European Journal of Information Systems*, **16(4)**, 327-335.
JENKINS A, ANANDARAJAN M and D'OVIDIO R (2014) 'All that glitters is not gold': The role of impression management in data breach notification. *Western Journal of Communication,* **78(3)**, 337-357.
KALGIN A (2016) Implementation of performance management in regional government in Russia: evidence of data manipulation. *Public Management Review,* **18(1)**, 110-138.
KANE EJ (2010) Redefining and containing systemic risk. *Atlantic Economic Journal,* **38(3)**, 251-264.
KATZ, R. L. AND KOUTROUMPIS, P. (2013). Measuring digitization: A growth and welfare multi multiplier. *Technovation*, ***33*(10-11)**, 314-319.
KEOHANE K (1998) Reflexive modernization and systematically distorted communications: an analysis of an Environmental Protection Agency hearing. *Irish Journal of Sociology,* **8(1)**, 71-92.
KLEIN HK. (1981). Design ideals and their critical reconstruction. In *Proceedings of The Institute of Management Sciences,* (pp. 12-26).
KLING R. (1978). Value conflicts and social choice in electronic funds transfer system developments. *Communications of the ACM*, ***21*(8)**, 642-657.
KNIGHT A. and SAXBY S. (2014) Identity crisis: Global challenges of identity protection in a networked world. *Computer Law & Security Review,* **30(6)**, 617-632.
KVASNY L and TRUEX D (2001) *Defining away the digital divide: A content analysis of institutional influences on popular representations of technology.* Boston, MA.
LAZONICK W and MAZZUCATO M (2013) The risk-reward nexus in the innovation-inequality relationship: Who takes the risks? Who gets the rewards? *Industrial and Corporate Change,* **22(4)**, 1093-1128.
LIN C-J (2007) Projected gradient methods for nonnegative matrix factorization. *Neural computation,* **19(10)**, 2756-2779.
LUHMANN N. (2005). Risk: A Sociological Theory. New Jersey: Transaction Publishers.
LUNDGREN, R.E. and MCMAKIN, A. H. (2018). *Risk communication: A handbook for communicating environmental, safety, and health risks*. John Wiley & Sons.
LUPTON D (2016) Digital risk society, in Burgess, Alemanno, and Zinn (eds.) *The Routledge handbook of risk studies*, Routledge, Taylor & Francis, pp. 301-309.
LYON D (2013) *The information society: Issues and illusions.* John Wiley & Sons.
LYON D (2017) Digital citizenship and surveillance| surveillance culture: Engagement, exposure, and ethics in digital modernity. *International Journal of Communication, **11***, 824-842.
MA SK (2018). *Modern theory of critical phenomena*. Routledge.
MADSEN C and KRÆMMERGAARD P (2015) The efficiency of freedom: Single parents' domestication of mandatory e-government channels. *Government Information,* **32(4)**, 380-388.
MAJCHRZAK A, MARKUS ML and WAREHAM J (2016) Designing for digital transformation: Lessons for

information systems research from the study of ICT and societal challenges. *MIS quarterly,* **40(2)**, 267-277.

MATHEWS L (2019) Louisiana Governor Declares State of Emergency After Ransomware Hits School Systems. *Forbes*. September 2019 https://www.forbes.com/sites/leemathews/2019/07/26/louisiana-governor-declares-state-of- emergency-after-ransomware-hits-school-systems/#20b361a8b37a

MIRANDA SM, YOUNG A and YETGIN E (2016) Are social media emancipatory or hegemonic? Societal effects of mass media digitization in the case of the SOPA discourse. *MIS quarterly,* **40(2)**, 303-329.

MIREA M, WANG V and JUNG J (2019) The not so dark side of the darknet: a qualitative study. *Security Journal,* **32(2)**, 102-118.

MISURACA G, PASI G and VISCUSI G (2018) Social Innovation and Resilience: Exploring the dynamics and impact on the digital transformation of governance & society. *Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance*.

MOROZOV, E. (2013), *To Save Everything, Click Here: Technology, Solutionism, and the Urge To Fix Problems That Don't Exist*, London, Penguin.

MYERS, M. D. (1994). A disaster for everyone to see: an interpretive analysis of a failed IS project. *Accounting, Management and Information Technologies*, *4*(4), 185-201.

MYERS MD. & KLEIN HK. (2011). A set of principles for conducting critical research in information systems. *MIS quarterly*, 35(1), 17-36.

NAM T (2017) A tool for liberty or oppression? A cross-national study of the Internet's influence on democracy. *Telematics and Informatics,* **34(5)**, 538-549.

NGWENYAMA O and KLEIN S (2018) Phronesis, argumentation and puzzle solving in IS research: illustrating an approach to phronetic IS research practice. *European Journal of Information Systems,* **27(3)**, 347-366.

NGWENYAMA OK and LEE AS (1997) Communication richness in electronic mail: Critical social theory and the contextuality of meaning. *MIS quarterly*, **21(2)**, 145-167.

NIELSEN FÅ (2011) *A new ANEW: Evaluation of a work list for sentiment analysis in microblogs.* arXiv preprint arXiv: 1103.2903.

OLSSON T (2006) Appropriating civic information and communication technology: a critical study of Swedish ICT policy visions. *New Media & Society,* **8(4)**, 611-627.

OPPERHUIZEN, A. E., PAGIOTTI, S., & ESHUIS, J. (2020). The roles of news media as democratic fora, agenda setters, and strategic instruments in risk governance: A double international case study on earthquake risk. *Journal of Risk Research,* 1-15.

PARK S (2019) Why information security law has been ineffective in addressing security vulnerabilities: Evidence from California data breach notifications and relevant court and government records. *International Review of Law and Economics,* **58**, 132-145.

RASMUSSEN MV (2006) *The risk society at war: terror, technology and strategy in the twenty-first century.* Cambridge: Cambridge University Press.

REUTERS (2016) *Digital News Report.* http://www.digitalnewsreport.org/survey/2016/denmark- 2016/

ROBINSON WI (2018) The next economic crisis: digital capitalism and global police state. *Race & Class,* **60(1)**, 77-92.

ROOZENBEEK J and VAN DER LINDEN S (2019) The fake news game: actively inoculating against the risk of misinformation. *Journal of Risk Research*, **22(5)**, 570-580.

ROSLYNG, M. M., & ESKJÆR, M. F. (2017). Mediatised risk culture: News coverage of risk technologies. *Health, Risk & Society*, ***19*(3-4)**, 112-129.

ROWE F (2018) Being critical is good, but better with philosophy! From digital transformation and values to the future of IS research. *European Journal of Information Systems,* **27(3)**, 380-393.

ROWE F, NGWENYAMA O, and RICHET, JL. (2020). Contact-tracing apps and alienation in the age of COVID-19. *European Journal of Information Systems*, 1-18. https://doi.org/10.1080/0960085X.2020.1803155

SCHULTZE U (2017) What kind of world do we want to help make with our theories? *Information and Organization,* **27(1)**, 60-66.

SEYD B (2015) How do citizens evaluate public officials? The role of performance and expectations on

political trust. *Political Studies,* **63**, 73-90.
SIMONOV, A., SACHER, S. K., DUBÉ, J. P. H., & BISWAS, S. (2020). The persuasive effect of fox news: non-compliance with social distancing during the covid-19 pandemic (No. w27237). National Bureau of Economic Research.
SLOAN RH and WARNER R (2019) *Why Don't We Defend Better? Data Breaches, Risk Management, and Public Policy.* CRC Press.
SLOVIC P (1993) Perceived risk, trust, and democracy. *Risk analysis,* **13(6)**, 675-682.
STAHL WA (1995) Venerating the black box: Magic in media discourse on technology. *Science, technology, & human values,* **20(2)**, 234-258.
STATISTICS DENMARK (2010) https://www.dst.dk/en
STREET CT & WARD KW. (2012) Improving validity and reliability in longitudinal case study timelines. *European Journal of Information Systems,* ***21*****(2)**, 160–175.
SUNDBERG L (2019) Electronic government: Towards e-democracy or democracy at risk? *Safety science*, **118**, 22-32.
TAKASHIMA R, YAGI K and TAKAMORI H (2010) Government guarantees and risk sharing in public-private partnerships. *Review of Financial Economics,* **19(2)**, 78-83.
UNGAR S (2001) Moral panic versus the risk society: The implications of the changing sites of social anxiety. *The British journal of sociology,* **52(2)**, 271-291.
WALSH G, SHIU E, HASSAN L, HILLE P and TAKAHASHI I (2019) Fear of online consumer identity theft: Cross-country application and short scale development. *Information Systems Frontiers,* **21(6)**, 1251-1264.
WHITLEY EA and HOSEIN I (2005) Policy discourse and data retention: The technology politics of surveillance in the United Kingdom. *Telecommunications policy,* **29(11)**, 857-874.
WHITLEY EA and HOSEIN I (2008) Doing the politics of technological decision making: due process and the debate about identity cards in the UK. *European journal of information systems,* **17(6)**, 668-677.
WILLIAMS R and EDGE D (1996) The social shaping of technology. *Research policy,* **25(6)**, 865-899.
WIRTZ, B. W., & WEYERER, J. C. (2017). Cyberterrorism and cyber attacks in the public sector: How public administration copes with digital threats. *International Journal of Public Administration,* **40(13)**, 1085-1100.
WRIGHT SA AND XIE G-X (2019) Perceived Privacy Violation: Exploring the Malleability of Privacy Expectations. *Journal of Business Ethics*, **156(1)**, 123-140.
YATES J (2003) An interview with Ulrich Beck on fear and risk society. *The Hedgehog Review,* **5(3)**, 96-108.
YEARWORTH M and WHITE L (2013) The uses of qualitative data in multimethodology: Developing causal loop diagrams during the coding process. *European Journal of Operational Research,* **231(1)**, 151-161.
YILDIZ M and SAYLAM A (2013) E-government discourses: An inductive analysis. *Government Information Quarterly,* **30(2)**, 141-153.
ZAMORA A (2019) Making Room for Big Data: Web Scraping and an Affirmative Right to Access Publicly Available Information Online. *J. Bus. Entrepreneurship & L., 12*, 203.
ZUBOFF S (2019) Surveillance Capitalism and the Challenge of Collective Action. *New Labor Form,* **28(1)**, 10-29.

Name of newspaper	Political orientation/ Type	Circulation figures (week-days) (source Reuters, 2014)	Number included in sample
Berlingske	Centre-right	2009 = 103.000/ 2013 = 82.000	271
Jyllands-Posten	Right	2009 = 120.000/ 2013 = 85.000	255
Politiken	Centre-left	2009 = 108.000/ 2013 = 92.000	195
Ekstra Bladet	Tabloid	2009 = 84.000/ 2013 = 52.000	111
B.T.	Tabloid	2009 = 75.000/ 2013 = 53.000	75
Information	Left	2009 = 22.000/ 2013 = 20.000	29
		Total	936

Table 1: The empirical materials: article distribution across newspapers and circulation counts

Appendix A
Results of Thematic Analysis, Ranking of Themes, Ratios and Sentiment Scores

No	Themes (including first year of introduction)	No. of LttEs	No. of Articles	Ratio LttEs/ Articles	Sentiment LttEs	Sentiment articles
1	The introduction of the NemID signature (2009)	22	121	.18	.36	.55
2	A debate on usability, security and marginalization of citizens (2010)	117	255	.46	.19	.46
3	Visions related to the overall digitization strategy promoted by government (2010)	21	25	.84	.38	.68
4	Mobile payments with or without digital signature (2010)	2	40	.05	.50	.78
5	Identity theft and hacking (2010)	11	26	.42	.36	.50
6	Cyberattacks and crime (2010)	9	74	.12	.33	.54
7	Security issues related to the use of Java (2010)	5	36	.14	.20	.56
8	The sale of the service provider Nets (2011)	16	80	.20	.25	.53
9	The use of NemID for online gaming (2011)	0	38	.00	.00	.92
10	Leaked information to a tabloid magazine (2012)	1	37	.03	.00	.03
	Total	204	732	.30	.25	.52

Appendix B
Critical Events in Evolution of the Danish Digital Risk Society

Date	Events
1998	- The government establishes the Digital Denmark Committee
1999	- The Digital Denmark Committee publishes report 'Digital-Denmark – Conversion to the Network Society' outlining targets for the development of the digital society
2000	- The Ministry of Finance establishes the Committee for Digital Administration
2001	- The Committee for Digital Administration stresses the need for a coordinated eGovernment strategy
2001	- e-boks (later renamed digital post) is launched for transmitting and storing digital financial and official documents from public institutions
2003	- All Public Administrations are granted the right to send documents electronically to all other authorities and to demand that documents from other authorities be sent electronically
2004	- Denmark becomes the first country to adopt the Universal Business Language (UBL) as a standard for public sector eProcurement
2007	- The 'borger.dk' portal is launched and becomes the citizens single Internet entry point to all Danish public authorities
2010	- **May:** The Minister for Culture, Mr Per Stig Møller and the Minister for Science, Technology and Innovation, Ms Charlotte Sahl-Madsen decide to jointly mobilize DKK 21 million (approx. € 1.6 million) for the digitization of the national cultural heritage for 2010-2012 - **July:** Charlotte Sahl-Madsen, the Danish Minister for Science, Technology and Innovation launches 'NemID', the new digital signature, which gives Danes a single access to public and private digital self-service solutions
2011	- Ministry of Finance launches Agency for Digitization to transform Denmark into a flourishing digital society. - More than 3.2 million Danes use it NemID, with over 2.9 million using it for both banking and the public sector. - NemID was used 310 million times by 79 % of the adult population to access services in both the public and private sectors, and notably for Internet banking
2012	- The Danish Parliament passes legislation as part of its policy to make digital self-service mandatory in several government service areas - **June:** The Danish Parliament approves law for a Public Digital Post which gives public authorities 'the right to send digital-only messages, letters and documents to their digital letter boxes instead of paper-based letters via traditional post' - **June:** The Danish Parliament passes an amendment which makes the first of four planned "sets" of digital self-service solutions mandatory for citizens. - **December:** The first set of services are mandatory: change of address, payments for license, state educationloan, national health care card applications, EU health care card, admission to day care, elementary school, and after-school care
2013	- **December:** The second of four planned "sets" of digital self-service solutions becomes mandatory for citizens. This set of services include, among others, choosing a physician, application for free admission to day care and after-school care, reporting of rat infestation, passport application, and declaration of fatherhood
2014	- **November:** Digital Post becomes mandatory and automatic for all citizens (15 years and older) who had not actively opted out, expected to save the government around DKK 1 billion on postage - **December:** The third of four planned "sets" of digital self-service solutions to become mandatory becomes mandatory for citizens.
2015	- **December:** The four set of digital self-service solutions becomes mandatory for citizens

Appendix C

Illustration of empirical analysis of validity claim related to usability					
Examples of claims made in media	Source	Validity claim	Testing criteria	Evidence of distortion	Source
System is easy to use System provider explaining nothing is wrong with system but users are not using system correct System is subject to unfair critique	JP 02.07.2010, BER 02.02.2010 EB 06.10.2010 BT 16.09.2010	SC	Logical consistency	Citizens find it complicated to use Elderly find it impossible to use Eighteen months after launch: The DaneAge association provide help and support to learn to use the system Elected politician refuses to use the system	JP 04.11.2010 JP 03.10.2010 BER 15.04.2012 EB 16.09.2010
System represents modernization of society System provider explains that citizens' equipment is not updated sufficiently	JP/ BER 02.07.2010 EB 06.10.2010 EB 08.10.2010	CC	Hyperbole or jargon	Citizens find it awkward to use both a paper based key and a digital key when logging into their vital online services Citizens are puzzled about detailed requirements to their PC	BT 05.07.2010 JP 06.07.2010 BER 31.07.2010 JP 25.09.2010
System is safe and reliable	POL 02.07.2010 BT 07.07.2010	TC	Falsehood	The system breaks down due to overload The system cannot respond fast enough to needs – citizens experience problems with unpaid bills Experts question the robustness of the system	BT 02.07.2010 BER 16.07.2010 EB 06.10.2010 POL 03.07.2010
Illustration of empirical analysis of validity claim related to vulnerability and hacking					
Examples of claims made in media	Source	Validity claim	Testing criteria	Evidence of distortion	Source
System is safe and reliable	JP 02.07.2010,	SC	Hyperbole and jargon	Experts and researchers challenge the safety of the system and provide examples of weaknesses The director of the Danish ITC Industry Association highlights the vulnerability of society by mentioning how everything is connected- exemplified by the risk of respirators in hospitals The ordinary citizen is left out of the debate due to the technical lingo (for example third-part software and malware)	BER 02.02.2010 JP 31.07.2013 BT 17.04.2013 POL 23.04.2013 JP 16.04.2013

				Hacking of central institutions including NemID and parliament An attack is done by teen-agers to expose the vulnerability which stimulate the fears of citizens	BT 12.04.2013 JP 10.07.2013
Revelation of silence about hacking from officials on purpose to avoid fears	POL 14.09.2010	TC	Incomplete statements	The public is not informed about dangerous hacking events. The silence concerning hacking is repeated by a politician years after the incident The NemID supplier admits that they were not well prepared for preventing attacks, but assures that it works 99% of the time	POL 15.09.2010 BER 08.06.2013 EB 18.10.2013
Banks calming by stating that hacking have no practical implications – data is not lost	BT 12.04.2013	LC	Assurance from authorities	Public does not receive full explanation of risks due to hacking	POL 14.09.2010
DDoS attack does not represent a threat to private data	BT 12.04.2013	SC	Connotative language	Discussions of whether or not cyber-attacks are criminal activities	JP 14.07.2013 JP 15.07.2013
Illustration of empirical analysis of validity claim related to sale of infrastructure					
Examples of claims made in media	Source	Validity claim	Testing criteria	Evidence of distortion	Source
Sale of infrastructure beneficial and necessary for Nets	BER 18.06.2013	TC	Incomplete statements	Concerns about sale could lead to access to confidential data	BER 19.06.2013 EB 20.06.2013 BER 17.02.2014
Communication about sale is driven by legal explanations about for example data protection laws	BER 18.02.2014	CC	Is communication intelligible?	Many opposition politicians point out the security dangers of a sale, but officials fail to acknowledge the issues	BER 08.06.2013 BER 13.02.2013
Discourse dominated by business analysts and financial experts emphasizing financial benefits and functioning of capital funds	JP 31.12.2013	LC	Are there undisclosed interests?	Citizens recall the role of Goldman Sachs in the financial crisis	JP 03.01.2014