Privacy in e-government 2.0. The case of Utrecht

Maurice Reedijk

458294

18-06-2017

Abstract

As local e-governments are transitioning towards the model of e-government 2.0, they are increasing their technological capabilities for collecting and analyzing data, making privacy issues become more apparent. Little scientific attention has been given to the privacy complications of e-government 2.0, and it mostly aimed at the benefits of the concept. Document analysis, interviews and participant observations are performed to determine how privacy is managed within Utrecht's e-government 2.0 design. The analysis shows that two recurring dimensions have played a crucial role in protecting citizens' privacy: awareness and transparency. Awareness embodies a conscious state of mind, is especially important with respect to the components of framework and data. Since e-governments operate in a digital context, perfect security does not exist. As mistakes are inevitable, the dimension of transparency represents the idea that trust of citizens' has to be maintained by being open about mistakes. In addition, when e-governments are transparent about which data is collected and for which purpose, privacy concerns among citizens will be reduced. The largest threat to privacy in Utrecht's e-government 2.0 is (a lack of) information security. Local municipalities, such as Utrecht, have the weakest information security of all government institutions, making them vulnerable to attacks from outside. However, the data of Utrecht's e-government remains relatively unprofitable for hackers, making the chances of specified hacks unlikely. This thesis has shown that in Utrecht's transition towards e-government 2.0, privacy has obtained a more pivotal role by incorporating awareness and transparency.

Keywords: *Privacy, E-government 2.0, Technology, Awareness, Transparency*

1. Introduction

In the last decade, there has been a rise of electronic governments (e-governments) within public organizations and public administrations around the globe. Historically, governments were seen as inefficient because they had little incentive to please the citizen, mostly due to the lack of alternatives for the citizen. However, the increase in technology and communication made an attitudinal change possible in which governments look at citizens like consumers that they have to satisfy (Evans & Yen, 2005). In order to do so, governments have been increasingly applying information and communication technologies such as the Internet and web-based networks to provide better services between government agencies, citizens, businesses, employees and other non-governmental agencies (Fang, 2002). The application of these new information and communication technologies by government became defined as e-government (1.0). This e-government model served a variety of different ends: better delivery of government services towards its citizens, better interactions between business and industry, and the empowerment of citizen through the provision of information and efficient government management (Basu, 2004).

Recently, due to the fast pace of technological innovations the technology of traditional e-government has been outpaced and led to the creation of the concept of e-government 2.0. Whereas the traditional e-government emphasized the automation of routine government operations for more efficiency and service, e-government 2.0 entails the incorporation of Web 2.0 technologies such as social media and networking sites for its digital activities. The application of social media technologies should be able to stimulate new forms of interactions that may result in improved communication and citizen participation, enhance citizens' trust in government as well as to enable them to make a contribution to public policies (Veljković, Bogdanović-Dinić & Stoimenov, 2012; Picazo-Vela, Gutiérrez-Martínez & Luna-Reyes, 2012). In other words, e-government 2.0 shifts the focus of citizens as not only users but also as active contributors to e-government.

However, there are still many gaps in the academic literature in regard to how these new technologies of e-government 2.0 are proposing to deal with the challenges and risks that are already present within the traditional form of e-government (Boersma, Meijer & Wagenaar, 2009). One of the major gaps, representing the largest threat that e-government poses for citizens, is endangerment of informational privacy. Informational privacy is the right to privacy of one's personal information, including information about one's actions, and the deliberate invasion of that privacy by the state (Bannister, 2005). Informational privacy is considered one of the key factors for insulating citizens from governmental tyranny and to

ensure the general health of liberal democracy (Waldo, Lin & Millett, 2007). The incorporation of Web 2.0 technologies will result in governments increasingly becoming more capable of storing and collecting new diverse forms of information and possibly jeopardizing the human right to informational privacy. When the amount of stored data becomes larger, it will be harder to adequately secure and anonymize the data (Narayanan & Shmatikov, 2006). As technological advancements are expanding the capabilities of conducting mass surveillance, the right to privacy will equally become more and more significant (Klitou, 2014). This shows that the emergence of e-government 2.0 not only poses certain academic questions, but also raises potential risks for individuals and society as a whole.

The aim of this thesis is to contribute to the academic field by explicitly examining how the concept of privacy unfolds itself within the framework of a local e-government 2.0. More specifically, it will scientifically determine the role of privacy in e-government 2.0 by conducting a case study on the e-government of Utrecht, the fourth largest city in the Netherlands. Utrecht was chosen because the Netherlands is ranked 7th worldwide on the United Nations e-government development index (UN, 2016). Utrecht is also one of the more digitalized local governments of the Netherlands, transitioning towards e-government 2.0 by incorporating Web 2.0 technologies and other new forms of interactive platforms. From all the cities in the Netherlands, Utrecht scores the highest on social media service. Besides the benefits for citizen-government interactions, this also means that Utrecht's e-government will be capable to increasingly obtain and store more data about its citizens. It will be interesting to determine how privacy is treated in a developing local e-government 2.0. This leads to the following research question:

How does Utrecht's e-government 2.0 design manage information privacy as it becomes increasingly capable of storing and collecting large quantities data?

2. E-government (2.0): Literature review

2.1 The historical development of e-government.

The introduction of the World Wide Web in the 1990s was the starting point of the concept of E-government. As the public adopted the Internet for personal use, the concept of e-government became the logical extension of the Internet for governments (Evans & Yen, 2005). Before the widespread use of the Internet, information technology use in government was primarily internal and managerial. Bozeman and Bretschneider (1986) were one of the academic pioneers that argued that technology is transforming the government and therefore called for more academic attention within this area.

The actual starting point of the implementation of e-government within the developed world occurred at a similar timeframe. In the United States, the culminated legislative efforts that occurred in the period between the 1990s-2000s eventually led to the enactment of the 2001 E-Government Act. This act provided both the organizational and financial infrastructure for the widespread use of e-government applications (Schelin, 2003). In 2000, the European Union initiative for e-government was initiated that consisted of four main tasks: development of Internet-based services to improve access to public information and services; improvement of transparency of public administration by using the Internet; and full exploitation of information technology within public administration and establishing e-procurement (Strejcek & Theil, 2002).

The tragic events of September 11, 2001, caused a major shift in the perception of the role of e-government. According to Halchin (2004), e-government shifted from a tool that was aimed at increasing efficiency and convenience of government services towards a tool of defense against terrorist threats. In the United States (but also in other countries) the government silently started to use the gathered data for data mining practices in name of national security. Furthermore, it reduced its safeguards against the collection, integration, and interagency sharing of private personal information. This new governmental approach undermined the privacy rights of its citizens and raised questions on the legitimacy of information use (Feinberg, 2004). Although the new concerns regarding this new adopted defense approach, the rise of e-governments and their applications kept growing. In 2014 the Organization of Economic Development (OECD) published a policy recommendation that urged all membership nations to embrace e-government as a means of reforming public administration and achieving broader policy objectives (OECD, 2014).

2.2 The emergence of e-government 2.0

The fast pace of technological innovations in recent years has led to the creation of new interactive technological tools, also referred to as Web 2.0 applications (Veljković, Bogdanovic-Dinic & Stoimenov, 2012). Web 2.0 refers to the new generation of Internet applications that are primarily aimed at collaboration and sharing information online such as social networks, blogs, and wikis (Veljković et al., 2012). The incorporation of these Web 2.0 technologies has produced a new ‘version’ of e-government, namely e-government 2.0. This version of e-government is specifically aimed at applying Web 2.0 technologies and other interactive Internet tools for creating new links and relationships between governments, citizens and innovative companies (O’Reilly, 2009). In other words, Web 2.0 applications are

not only affecting the way how people communicate with one another, but they also bring changes to how interaction takes place with the government.

According to Sivarajah, Weerakkody, and Irani (2016), the application of these new technologies is supposed to strengthen government legitimacy as well as to boost the efficiency and effectiveness of government policies. Governments will be able to tap into the intelligence of the crowd through using Web 2.0 technologies. New interactions are expected to enhance citizens' trust in government as well as to enable them to make a contribution to public policies. Veljković et al. (2012) also argue that e-government 2.0 involves a shift towards a culture of openness and transparency. This means that the government is prepared to engage and listen to its citizens and to make non-sensitive public sector information available for consumption.

Yet, one could question whether, and to what extent, these expectations are realistic. Countering the promising Web 2.0 stories, Norris (2010) argues that, despite all technological developments, a greater degree of interactivity or more e-participation or democracy cannot be expected. He argues that the positive hype around e-government 2.0 is dangerous, since these new technologies are being framed as value free and inevitable. Utopian stories about new technologies may, therefore, hamper public debate about the benefits and drawbacks (Meijer et al., 2009).

2.3 E-government: definition and growth model

Although there is no clear universally established definition of the concept of e-government, in this thesis e-government will be defined as "the continuous optimization of service delivery, constituency participation, and governance by transforming internal and external relationships through technology, the Internet, and new media."(Fang, 2002, p3).

Like any other large-scale system, e-government is often examined through the use of development models that outline a number of stages that occur when government structures and functions transition towards e-government (Nour, AbdelRahman & Fadlalla, 2008). There are a great variety of e-government development models that all seem to be incongruent to each other, employing different perspective and stages. In order to develop a common frame of reference, Lee (2010) conducted a qualitative meta-synthesis of all the existing development models. This meta-model of e-government consists of five metaphorical stages: presenting, assimilating, reforming, morphing and e-governance. Each stage is viewed from two separate perspectives, namely the citizen/service perspective and operation/technology perspective. This means that within each stage, there are two elementary concepts that are

linked to a specific perspective, with the exception of the first stage that only has one elementary concept that can be used for both perspectives (see Table 1).

Table 1*: Overview of the stages of e-government*

Metaphors	**Descriptions**	**Stages/concepts**	
		Citizen and service	Operation and technology
Presenting	Present information in the information space	Information	Information
Assimilating	Assimilates or replicates processes and services in the information space with in the real world	Interaction	Integration
Reforming	Reform processes and services in the real world to match information space requirements, aimed at efficiency	Transaction	Streamlining
Morphing	Change the shape and scope of processes and services in both the information space and the real world	Participation	Transformation
e-Governance	Processes and service in both worlds are influenced by input of citizens	Involvement	Process management

This table is taken from Lee (2010, Table 3).

Application of Lee's model to Utrecht's e-government.

This growth model has been applied to Utrecht's e-government to determine its stage of implementation of e-government 2.0. The metaphorical stage *presenting* refers to the simple presentation of information, without any additional functionality. This stage includes cataloging, publishing, scattered information, and billboards. This stage is clearly present in Utrecht. The website of Utrecht provides extensive digital information on a lot of different topics, such as housing, healthcare, education, jobs, regulations, security, environment and so forth.

The second stage, *assimilating* (interaction and integration), is also present in the digital environment of Utrecht. This stage entails the emergence of interaction based services

which makes two-way communication between government and citizens is possible (Lee, 2010). The digital environment of Utrecht offers the opportunity for citizens to interact with the local government by means of digital communication. On the website, citizens can file complaints, ask questions and request more information. Besides communication through the website, Utrecht has also started to use social media as interaction tool. It is now possible to interact with the government of Utrecht by Twitter, Facebook, Instagram and more.

The third stage, *reforming (*transaction and streamlining), is also incorporated in the e-government of Utrecht. Transaction revolves around the idea that the ways in which the government does business with its citizens are reformed. This stage opens up the ability for citizens to perform financial and service transactions in a digital and more efficient matter. On the other side, it involves streamlining governmental business- and service processes by means of information technologies and systems (Lee, 2010). In the past, citizens had to physically visit the municipality of Utrecht when they wanted to register themselves, apply for permits and social grants and requesting ID-cards. At this moment, all these transactions can be done digitally.

The fourth stage entails *morphing (*transformation and participation). This stage revolves around the idea that the streamlining of transaction capabilities opens up the ability for citizens and officials to see completely new possibilities in the configuration of services and processes. This stage can also be witnessed in Utrecht, where the government of Utrecht just initiated new projects such as Participedia, Jij Maakt Utrecht (JMU) and Open Data. The Participedia and JMU are new projects that are trying to involve citizens in policy-making and giving them the opportunity to collaborate with local business, other citizens and the local government to initiate their own projects, ideas or other initiatives. The Open Data platform is a project that provides (anonymized) governmental data that will be accessible for everyone, with the idea that this information might be fruitful for businesses, organizations, journalists, researchers, and citizens.

The last stage, *e-Governance* (process management and involvement) is closely related to the previous stage. This stage requires e-governments to reconfigure business processes of administrative and political services based on real-time contributions of citizens. It requires citizens to have actual involvement in decision-makings of the government in real-time. The projects of Participedia and JMU are f examples in which real-time suggestions and adjustments can be made, it is not clear whether policy-makers also incorporate these suggestions and adjustments in real-time.

Overall, Utrecht can be considered an e-government 2.0. As discussed in the

interaction stage, the government of Utrecht is applying Web 2.0 technologies as means for information provision and communication with its citizens. The use of social media as communication service has been rising steadily within the e-government of Utrecht (WistUdata, 2016). Additionally, the projects of JMU, Participedia and Open Government can also be considered forms of Web 2.0 technologies. Nevertheless, the question still remains how Utrecht's e-government aims to maintain privacy in spite of incorporating these new technologies.

3. Privacy: Literature review

3.1 Privacy: concept and definition

Privacy, like the freedom of speech, is a fundamental human right that is recognized in the United Nations Declaration of Human Rights (Gritzalis, 2004). However, although privacy is a fundamental right, the concept of privacy remains ill-defined but well-understood. Privacy is well-understood in the sense that most people do have an idea or opinion about what privacy entails. On the other hand, privacy is ill-defined, because it is hard to find a definition of privacy in the academic literature that is straightforward (Introna & Pouloudi, 1999; Waldo et al., 2007). There is no logically consistent "umbrella" theory of privacy, but the concept is subjected to ''inherent flexibility'', meaning that the definition of privacy and the belief in its importance or value differs between people based on their personalities, experiences, interests, occupation, and status within society (Klitou, 2014; Waldo et al., 2007).

Nevertheless, it is possible to outline the underlying concept of privacy. Historically in Europe and North America, and based on the Fourth Amendment of the US Constitution, the right of privacy is seen as a defense against any "unreasonable" physical intrusion upon one's private home, private papers, personal belongings and one's body (Klitou, 2014). Over the years, the legal and societal definition of the concept has broadened to encompass various types of information that could be available about an individual. These types of information include behavioral, financial, medical, biometric, consumer, and biographical. Additionally, privacy also constitutes information that is derived from the analysis. This means that privacy interests are also linked to the gathering, control, protection, and use of information about individuals and the deliberate invasion of those privacy interests by the state (Waldo et al., 2007; Klitou, 2014; Cate, 2002; Bannister, 2005). These informational dimensions of privacy will constitute the definitional center for this thesis.

3.2 Is privacy important?

The importance of informational privacy is equally as fluid as its academic definition. The

importance of privacy as a fundamental right has been subjected to philosophical, sociological, psychological and legal explorations. Westin (1967) is considered one of the most influential pioneers who constructed the very first formulations of so-called informational privacy. Westin (1967) conducted an interdisciplinary approach to the nature and functions of informational privacy, and his overall theory of informational privacy is still adopted by scholars in this information age (Waldo et al, 2007; Westin, 1967; Whitley, 2009).

In his theory, Westin (1967) describes four distinct states of privacy: solitude (freedom from observation), intimacy (closeness among a small group of people), anonymity (freedom from being identified in public settings), and reserve (freedom to withdraw from communication). These states are subject to constant change, depending on one's personal needs and choices about what to reveal and what not to reveal at a given time (Westin, 1967). According to Westin (1967), the importance of this control over information disclosure is crucial for an individual's self-development and its ability to exercise responsible citizenship. Based on his constructs and concepts, the claim is made that privacy is a fundamental part of civil liberty within a democratic society.

On the other hand, many people say they are not worried when the government gathers or analyzes personal information. After the Snowden leaks in 2013 that provided unprecedented insights into the workings of state corporate surveillance programs based on the interception and collection of online activity, there has been little evidence of public outcry, with often conflicting and inconsistent opinions on the subject (Dencik & Cable, 2017). When the government engages in surveillance, many people believe that there is no threat to privacy unless the government uncovers unlawful activity, in which case a person has no legitimate justification to claim that it remain private (Solove, 2007). The "nothing to hide" argument and its variants are quite prevalent in popular discourse about privacy, and in its most compelling form, it is an argument that the privacy interest is generally minimal to trivial, thus making the balance against security concerns a foreordained victory for security.

However, there are various examples in which seemingly trivial data turned out to be a dangerous and powerful tool. Seltzer (1998) shows that the population register played a crucial role in the systematic killing of Jews during the Second World War. The data from these population registers were used to obtain information about the number of Jews, where they lived, how many family members they had and so forth. This shows that potential misuse and/or abuse of major (trivial) data systems by aggressively malevolent governments may have severe consequences. Although much has happened since that time, and several protective legislation has been put in place, it remains fair to question how these protective

measures will adequately deal with more widespread, systematic, and malevolent threats, including domestic tyranny or external occupation (Seltzer, 1998).

3.3 Privacy in a digital era

In the last decades we have witnessed immense advancements of information and communications technologies, and these technologies have dramatically transformed our way of life (Solove, 2004; Gritzalis, 2004). The personal computer, for example, has evolved from a simple typewriter to an entry point to a network of global scope. The computer is now utilized for a variety of reasons, such as personal interactions, financial transactions, gathering information, and entertainment (Waldo et al., 2007). These developments occurred so quick and ubiquitous that the protection and importance privacy in this digital era has become very complex. The use of these online technology allows for faster, easier storage of more data, aggregation of that data and all that without the consumers' knowledge (Gritzalis, 2004). This ignorance and complexity make it hard for societies and individuals to adequately evaluate the extent to which governments and commercial companies are able to pry into their private affairs and the consequences that it might bring. Although the use of online technology has fired up some privacy concerns, these concerns are often outweighed by the advantages for customers, citizens, and businesses. The collection of data allows personalization and customization of the consumer's interaction with (governmental) organizations or businesses, and the use of information technologies has become an important tool for all types of organizations to improve their efficiency. According to Sweat (2002), consumers often agree that giving personal information on the web is beneficial if it means they will get better service, convenience, or benefits on that particular website.

The complexity of this digital era creates a situation in which it is very difficult to establish a coherent juridical framework. The rapidity of the technological developments makes it hard for official legislation to transition and evolve fast enough, and may fall short for the decades to come (Van Zoonen, 2016). Existing regulatory schemes are incapable of keeping pace with these norms and practices (Crawford & Schultz, 2014). Decisions, legislation, and discussions that are revolved around privacy are therefore crucial, because societies risk stumbling into a situation which may be difficult to reverse (Bannister, 2005).

Van Zoonen (2016) has constructed a privacy framework that is aimed at determining what privacy concerns among citizens are produced in the context of local e-governments. The framework consists of two main dimensions (data and privacy), where the data axis runs from personal to impersonal data and the purpose dimension axis depicts the difference in

purpose for which data is collected, ranging from service to surveillance purposes (see Figure 1). The broadness of these dimensions makes the framework applicable to every separate stage of e-government, because the purpose and type of data are relevant in all stages. When applying these two dimensions in a matrix, four quadrants come up: personal data for service (I); personal data for surveillance (II); impersonal data for surveillance (III) and impersonal data for service (IV) (see Figure 1). Van Zoonen (2016) argues that based on existing research about privacy perceptions, the privacy concerns of citizens are lowest when impersonal data is used for service purpose, while privacy concerns are highest when personal data is used for surveillance purposes.

In the case of Utrecht, the framework of Van Zoonen (2016) may be particularly useful in Utrecht's process of incorporating the latest stages (morphing and e-Governance) of Lee's (2010) e-government model. The framework can serve as a sensitizing instrument for policymakers and operational managers to conceptualize how privacy concerns among citizens will occur when designing new technological services.

Figure 1: *Framework of privacy concerns in e-government.*

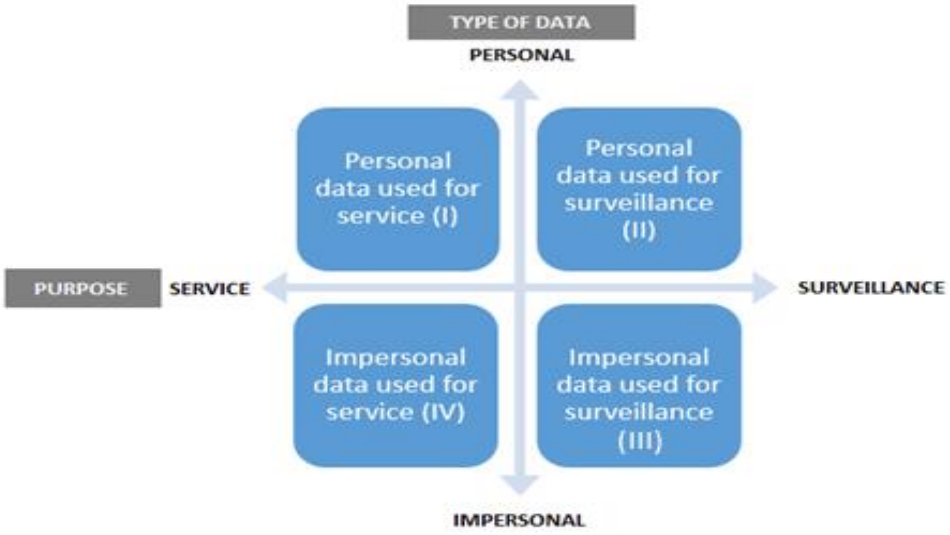


Figure taken from Van Zoonen (2016, Figure 1).

3.4 Privacy and Big Data analysis

As information systems are starting to move from isolated systems to clustered interconnected information and analysis systems, it has become easier to share and aggregate data. In recent years, there has been a lot of scientific attention to how these large datasets can offer new insights into previously intractable problems (Crawford & Schultz, 2014). The analysis of these new forms of data is usually referred to as "big data", which is an imprecise but

generalized term that refers to large data sets in data science and predictive analytics. Big Data is surrounded by the notion that large data sets generate results with greater truth, objectivity, and accuracy and therefore has the power to solve problems in numerous disciplines and business arenas (Crawford & Schultz, 2014). According to Kim, Trimi & Chung (2014), big-data applications can help governments to enhance their national security, fight global issues such as global warming and terrorist threats, and track down illegal activities like fraud.

However, alongside all of its promises, big data also presents serious privacy problems. As governments are increasingly applying big data methods, potential harms of enabling discriminatory housing practices, exposing sensitive health information, and facilitating predictive policing become apparent (Crawford & Schultz, 2014). The companies that are designing big data analysis software, admit that their systems do not necessarily conform to practical or ethical standards, and are not able to tell whether the results are right or not (Crawford & Schultz, 2014). Such unrestrained governmental power may be susceptible to abuse, endanger individuals' right to privacy, and weaken individuals' trust in government. If e-governments want to reap the benefits of big data without endangering citizens' privacy, they should focus on constructing and implementing safeguards that are aimed at maintaining privacy.

3.5 Privacy-enhancing technologies and regulations: What strategies are there?

Although in the previous sections it can be seen that technology has the potential to threaten privacy, it is not inherently destructive of privacy. Technological developments can also contribute to the enhancement of security and privacy, by limiting access or controlling the information that is collected about people. Besides technological developments, laws and/or regulations can also help to maintain our fundamental human right to privacy.

In this thesis, only privacy-enhancing technologies for information collectors will be discussed. Privacy-enhancing technologies for information collectors can be defined as a term which encapsulates all software, hardware and organizational measures which allow organizations to better protect the privacy of the customers they collect data from (De Roode, 2016). This section will discuss the major privacy-enhancing technologies that are including in the *General Data Protection Regulation* (GDPR), the most recent privacy regulation of the European Union (European Commission (EC), 2016).

The GDPR obligates organizations to perform a Privacy Impact Assessments (PIA) of technologies, services, and processes that have the potential to endanger informational rights

of the subject. PIA is an analysis of how personally identifiable information is collected, stored, protected, shared, and managed. The purpose of a PIA is to demonstrate that system owners and developers have consciously incorporated privacy protections throughout the entire lifecycle of a system. This involves making certain that privacy protections are built into the system from the start, not after the fact when they can be far more costly or could affect the viability of the project (Waldo et al., 2007). This definition of PIA is similar to the concept of privacy-by-design, which entails that organizations take privacy into account when developing products, services and information systems.

Furthermore, organizations are also required to implement measures that mitigate the risks of data leaks and security infringements (EC, 2016). Pseudonymisation is a possible tool to meet these data-protection obligations. Pseudonymisation refers to a technique in which identifying sensitive data is replaced by one or more pseudonyms. The key of the encryption is designed and maintained by a Trusted Third Party (TTP). The TTP is an external, trusted, reliable party which has no strong affiliation with the organization. This solution ensures that when the organization's database is leaked, it is not possible to directly relate all data to a person because the identifying data is encrypted and not readable without the encryption key (de Roode, 2016). When insufficient data protection measures have been taken, organizations can be severely fined, up to 100,000,000 euros. (EC, 2016).

Based on the latest stages of Lee's (2010) e-government model, the privacy-enhancing technologies included in the GDPR fit within the stage of morphing. It changes the shape and scope of the processes and services of e-governments to be more protective of privacy. It might be beneficial for Lee's (2010) e-government model to integrate privacy-enhancing technologies so that the level of required privacy maturity can be combined to the stages of e-government. Additionally, it is interesting to notice that the concepts of privacy-by-design and the PIA are pursuant to the framework of Van Zoonen (2016), substantiating the relation between data, purpose and technology/tools.

4. Methodology

In this section, the methodology used in this thesis will be discussed. The thesis has three main methods of research, namely document analysis, interviews and participant observation. This variety of qualitative methods has been chosen due to the current state of privacy and e-government, that is currently in implementation. By applying diverse methods, it will be possible to obtain multiple perspectives on the case within the relevant societal and technical contexts.

4.1 Document Analysis

Document analysis is a systematic procedure for reviewing or evaluating documents—both printed and electronic (computer-based and Internet-transmitted) material. Similar to other analytical methods in qualitative research, document analysis examines and interprets data in order to obtain a better understanding, elicit meaning and develop empirical knowledge (Corbin & Strauss, 2008; Rapley, 2007). Within document analysis, there is a distinction between primary-(generated by the research subjects) and secondary documents (academic literature). The analytic procedure of document analysis entails finding, selecting, appraising, and synthesizing data contained in primary documents. In document analysis, the data (excerpts, quotations, passages) are then organized into major themes, categories, and case examples specifically through content analysis (Labuschagne, 2003).

The primary documents that will be analyzed consist of four official governmental documents related to current policies and future ambitions of Utrecht's e-government. Examples of these documents are the '*Privacyverordening Gemeente Utrecht 2016'* (translated as: privacy regulation municipality of Utrecht and the "*Strategisch Informatiebeveiligingsbeleid Gemeente Utrecht 2014-2018" (*translated as: strategic information security policies). The municipality of Utrecht provides an online database (*iBabsonline)* which contains all official documents (memo's, questions, motions, reports, and amendments) that have been filed since 2007. I have used this database to search for information regarding the protection, collection, supervision, and control of citizens' privacy. For example, I conducted searches for words like privacy, digital government, online security, social media and other relevant terms.

Additionally, I also analyzed documents that, although part of the academic and popular literature on e-government and thus secondary documents, were produced by academics who are also important actors in the field of e-government. As such, these sources were treated as primary documents for the purposes of this study. Examples of these documents are the books "*Engaging privacy and information technology in a digital age*'' by Waldo, Lin and Millett (2007), "*Privacy-Invading Technologies and Privacy by Design*" by Demetrius Klitou (2014) and *"The digital person: privacy and technology in the information age"* by Daniel Solove (2004).

4.2 Interviews

The second method for research in this thesis consists of interviews. Interviews are a tool of social research in which communication is the core method of producing different forms of

information with individuals and groups (Bryne, 2004). Interviews offer access to interviewees' views, interpretations of events, understandings, experiences and opinions, and because they are more open to hearing respondents' views 'in their own words', it allows for a more complex analysis (Bryne, 2004). This new interaction between privacy and e-government is fairly complex, and therefore the inclusion of interviews as a research method seems very suitable. The interviews will be semi-structured, meaning that there are some core topics that will come back in every interview, but also offers the possibility to deviate from those topics when other interesting information comes out.

In total eight interviews were conducted, with the length of each interview lasting around 45 to 75 minutes. The e-government of Utrecht encompasses a large quantity of employees, organizations and other relevant stakeholders. In this thesis, I focused on obtaining a strategic sample of the core drivers behind the construction, implementation, and execution of privacy policies within Utrecht's e-government. Therefore, the goal was to have a representative sample of respondents within the field of informational privacy, the construction, and implementation of Utrecht's e-government privacy policies and the security of information systems. The diversity of respondents provides various perspectives on the topic. Additional information regarding the respondents is outlined in the appendix (appendix 8.1).

For informational privacy, two interviews were held with respondents that are related to organizations that are actively involved in the protection of privacy within the Netherlands. Both of these organizations have the goal to protect citizens' privacy rights and inform them about the possible risks that privacy infringements have. They also critically assess the privacy policies of national- and local governments.

Secondly, four respondents were interviewed who were actively involved in the development of Utrecht's e-government and privacy regulations. These respondents were chosen due to their proximity to the development of Utrecht's e-government and the privacy issues that this development has evoked.

Lastly, two respondents have been interviewed that have knowledge on the technological aspect of the electronic government and most importantly its electronic systems.

4.3 Participant observation

The third method that was used in this research was participant observation. Three various settings have been attended: a privacy practitioners community organized by the Centre of Information security and Privacy protection (CIP), a conference of Bits of Freedom and the

Correspondent on data usage in contemporary society and the examination of the live-streamed town council meeting of Utrecht's e-government on the privacy regulation of 2016.

This anthropological research method is useful for obtaining insight on nonverbal expressions of feelings, discourses, and implicit relations between actors (Neuman, 2012). By attending and participating in these three various settings, new perspectives on the issue were formed that did not come forward out the more formal interviews and documents.

5. Analysis: Model of privacy in Utrecht's e-government 2.0

The analysis of Utrecht's e-government 2.0 provides an interesting case study of how informational privacy can be treated within a digitalizing local government. By analyzing primary documents, interviews and participant observations a scheme linking all the concepts together has been constructed, identifying the most important concepts for maintaining privacy during Utrecht's e-government development (see Figure 2).

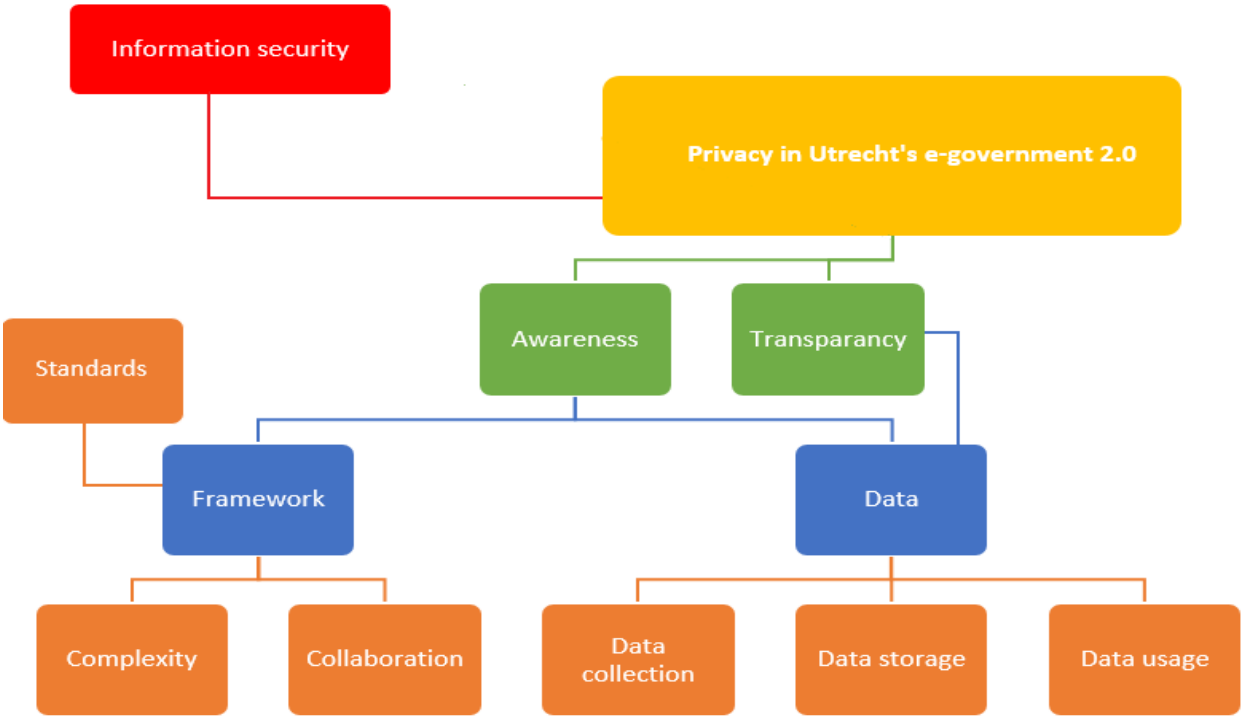
The starting point of the figure is privacy in e-government 2.0, which is one of the many dimensions that are present within an e-government. Information security positions itself next to the dimension of privacy, because information security is an independent dimension within e-government which has broader goals than only ensuring privacy. However, information security is important because is the first line of defense, meaning it affects all concepts and components that are present within the dimension of privacy.

Within privacy, I have identified two main concepts that my interview subjects indicate are crucial for maintaining privacy in Utrecht's e-government 2.0: *awareness* and *transparency*. Awareness is a broad concept that signifies a conscious state of mind that is well-informed about particular situations or developments, in this case, privacy. This awareness occurs within two distinct components that are connected to each other, framework and data. The framework component stands for the construction of a shared frame of reference regarding standards on data collection, usage, and storage. It also entails the need to unravel the complexity of privacy by collaborating with relevant stakeholders and exchanging best practices. Awareness with respect to the data component represents the belief that choices on data collection, storage and usage should be made consciously, with an understanding of their possible consequences.

Transparency has been identified as an essential concept for maintaining the trust of citizens, even when sensitive and personalized data is compromised. The privacy concern framework of Van Zoonen (2016) shows that the privacy concerns of citizens depend on the type of data that is collected and the purpose for which it is used. Therefore, the concept of

transparency is linked to the data component, because transparency can provide openness on the collection, storage, and usage of data and may subsequently diminish privacy concerns.

Figure 2*: Overview of my analysis model for privacy in e-government.*



5.1 Awareness

The technological developments that we have seen in the last decades and the utilization of technological tools in everyday life, the public sector, and private sector is surrounded by unawareness, incompetence, and disinterest. Technology is widely embraced by all aspects of society, but just a few manage to critically assess how technology and data works and what its possible consequences are.

In the context of privacy in e-government, the most prevalent reoccurring theme that comes out of my research is that of *awareness*. Lack of awareness seems to be involved in all aspects of privacy, from privacy protection to service enhancement, data collection, and analysis. The complexity and rapidity of technological developments and services have created a situation in which citizens, civil servants, policy-makers, and managers are simply not aware of what privacy entails, what data collection means, why data can be sensitive and how they should treat it. According to Suzanne Schilderman, council member of the municipality of Utrecht, insufficient knowledge about privacy and data is present in all organizations:

> "In essence, I think that every organization knows too less about this [read privacy and data treatment]. I have encountered a few organizations which made me say 'This is really good enough'. I believe that is because there is a lot of disinterest in what computers are, what data is and what happens with it". (Interview 3, council member).

Dimitri Gilissen, also a council member of the municipality of Utrecht agrees to this notion, stating that "the government and the municipality have started too late with creating awareness for civil servants that they should deal very carefully with privacy and sensitive information". Sijmen Ruwhof, an ethical hacker, takes a broader perspective. In his eyes, a lack of awareness is not something that is solely present in local e-governments, but that unawareness has a global character. No one seems to comprehend the dangers of the digitalizing world, and he compares the information technology to the financial sector, where things first have to go wrong before awareness will come and changes can be made.

> "It is not a question whether things will go wrong, but when they will go wrong. The situation has become too complex, too unclear. No one knows what they are doing, and everyone is simply occupied with applying quick fixes for short-term results instead of the long term. Only when things go wrong, it will become unpleasantly clear how bad our information security was". (Interview 1, ethical hacker).

Brenno de Winter, an IT-expert and investigative journalist, is not so sure whether incidents will help create awareness for privacy issues:

> "Large-scale incidents are already happening, that is the weird thing. It is not like we are currently in a situation where things go wrong now and then, no, incidents occur all the time that involve billions of personal data. Those are staggering amounts, and similar problems still reoccur". (Interview 4, IT expert).

Gilissen thinks that more attention to the negative aspects of technology will be given as soon as the consequences become greater. However, he argues that even if there is a lack of political and societal attention towards the implications of privacy in the digital context, the embracement of technological tools should not be hampered:

> "It is a wicked problem. Scientific unclarity and no societal consensus. Makes it hard for a political debate, and to construct policies. Policies are a simplification of problems that are present in society, but the current developments of privacy make it difficult to simplify. Does that mean we have to halter technological developments? No. Does that mean we have to become aware, and open our eyes and ears? Yes". (Interview 2, councilmember).

This quote shows that his solution to reap the benefits of technological advancements is by becoming aware. The idea of awareness not only came forward in the interviews, but also official documents of Utrecht's e-government and the European Union, council meetings, and

the newest privacy baselines constructed by CIP all highlight the importance of being 'aware'. When analyzing both the newest privacy regulation of Utrecht's local e-government, as well as the upcoming regulations of the European Union (GDPR), the Privacy Impact Assessment (PIA) and privacy-by-design are core concepts. Underlying motives of these concepts is to force policy-makers, managers, and employees to become aware of possible privacy implications. It requires actors to take privacy into account when engineering and constructing new processes and services. Another new requirement of the GDPR is that every government organization that has more than 150 employees have to appoint a privacy officer. Gilissen argues that appointing a privacy officer is not necessarily a solution to the problem:

> "You can appoint all kind of security and privacy officers, but eventually the responsibility of protecting citizens' privacy lies in every civil servant of Utrecht's e-government that works with privacy sensitive information, so it is important that they are aware of that. Creating awareness for them requires a lot more than simply appointing a privacy and security officer. (Interview 2, councilmember).

Schilderman creates a more nuanced perspective. She says that there is an uprising trend and that awareness of privacy implications is slowly becoming present in Utrecht's e-government.

> "I have the idea, that nowadays, there is more attention for privacy in the organization. More money has been cleared for privacy goals, so that is definitely an upwards trend. People have become more aware of working with data and can be seen in all aspects of the organization. It pleases me to hear that when the traffic department is discussing policies, immediately remarks regarding possible privacy implications are made." (Interview 3, councilmember).

Awareness has shown to be a key concept in the discussion revolved around privacy in a digital government, and on the newest technological developments in general. Ad Reuijl, director of CIP, agrees with Schilderman's observation that awareness within organizations is definitely in development. However, he does notice a difference between the public- and private sector:

> "There is definitely a development going on in terms of awareness in organizations, organizations start to reason from a responsibility perspective of someone else's data. This can be seen in both the public- as the private sector, but the private sector is doing a little bit better than government in terms of awareness. The market has both financial as exposure damage when things go wrong. The public sector on the other hand currently only has reputation damages (Interview 6, director of CIP).

The difference between market and public sector might disappear when the GDPR will be in place. The new legal privacy framework will also create severe financial consequences for government institutions when privacy is not rightfully considered.

5.1.1 Awareness in data

The contemporary technological advancements are primarily built around creating better service and efficiency by information systems that produce a lot of useful data that sustains the quest to obtain more efficiency. This new playing ground of technology and data created a platform in which the incorporation of technology in (local) governments is inevitable. Without technological tools, governments will not be able to transition accordingly with our contemporary society. Based on the primary documents and interviews, awareness is seen as the instrument that will help to make this incorporation of data collection, usage, and protection as reliable as possible. This becomes apparent when discussing the application of social media by the e-government of Utrecht. All respondents agree that social media is a useful tool for improving interaction with citizens (Interview 1, 2, 3, 4, 5, 6, 7, and 8). The risks of the use of social media, e.g. exchanging sensitive information, can be prevented if citizens, civil servants, and policy-makers are aware of the costs and benefits of the platform.

> "As long as you concretely consider for which purpose you use, then it can be an enrichment to the government and citizen. This part also contains the awareness, if the guidelines are good then it can definitely be an addition. But what you shouldn't do is use social media to exchange personal sensitive information like, citizen service numbers and so forth". (Interview 3, council member).

All my interview respondents argued that the incorporation of Web 2.0 technologies is inevitable for Utrecht's e-government if they want to compete (Interview 1, 2, 3, 4, 5, 6, 7, and 8). When discussing the possible negative effects of these new technologies, awareness is considered as the solution to reduce the privacy implications in the incorporation of Web 2.0 technologies such as social media, blogs, and wikis. The underlying idea is that by thinking about possible privacy implications, these new technological tools can be rightly adjusted so that Utrecht's e-government can use it without producing negative side effects. When a new service is implemented in Utrecht, assessments on the motives for data collection and usage have to be provided. Hans van Impelen, privacy officer of Utrecht, states that in expanding digital services data minimization has to be the starting point:

> "You have to be able to provide strong arguments to as why want to collect what you want to collect. Data minimization is the focus in Utrecht, you only collect data for the purpose it was meant for. Yes, it is possible to collect a lot nowadays, but if you only need an e-mail address, then just limit yourself to that". (Interview 5, privacy officer).

The collection of new forms of data, such as social media or tracking, is not necessarily problematic if those involved. The preconditions that are constructed in Utrecht's e-

government in terms of data collection, usage and protection seem to match the conditions of the privacy framework constructed by Van Zoonen (2016). The e-government of Utrecht anonymizes and/or pseudonymizes all the collected data, and uses this impersonal data to enhance the interaction with citizens, map social issues such as crime and debts, and improve traffic congestions. So how does Utrecht's e-government ensure that the collected data is impersonal and that it is primarily used for service enhancement? According to Van Impelen collected data has to be treated carefully by data analysts and scientists:

> "There is a team of data analysts and scientists, and we developed a structure in which we are able to obtain the valuable information out the collected data, without harming citizens' privacy. We do this by separating tasks and functions of organizational departments. Some departments are responsible for the execution of services, so they require personal and sensitive information, which is also required by law. But the analysis is done by a central team of data scientists that only receive anonymized or pseudonymized data. They do not need personal information, they only need to know descriptive information on certain neighborhoods, in order to map specific problems and/or needs. The results of these descriptive analyses are then given back to other organizational units to improve processes and policies". (Interview 5, privacy officer).

6.1.2 Awareness as a framework

Another component of privacy revolved around the concept of awareness is a local, national and supranational framework. When talking about the protection of privacy and data, you are as strong as your weakest link. In an e-government, data exchanges between other organizations occur very frequently. Even if you treat the security of privacy and data as an e-government very importantly, when data exchanges occur this security is not only in your hands anymore.

Most of the respondents have stated that it is therefore crucial that there is one global framework that explicates complex definitions and concepts such as what data is, how to define a data leak, what analytical techniques there are, how to perform privacy impact assessments and so forth (Interview 2,3,4,5,6 and 8). As stated in the framework section, it is important to use a similar framework because you are as strong as your weakest link. But besides having general rules and frames about how to treat privacy, you also need to collaborate to deal with threats. Privacy in the digital infrastructure is a highly complex and also a wicked problem, and it is therefore crucial to exchange fruitful information. The high-pace of technological developments and threats makes it vital to collaborate with partners and to share best practices.

Van Impelen acknowledges the importance of a shared collaborative framework and

the exchange of information. Utrecht's e-government collaborates with the Center of Information- and Privacy security (CIP), a network organization that shares their knowledge on privacy with its members, including guidelines, baselines, and privacy impact assessments templates. Hans van Impelen, the privacy officer of Utrecht's e-government, states:

> "The CIP is a network organization. I actually immediately became a member (when he got appointed as privacy officer), because I knew it will give multiple advantages. I regularly attend their privacy workgroup and often use their baseline of privacy models. Those are really nice things, because the same risks that we experience are experienced by others as well". (Interview 5, privacy officer).

The tools and information provided by CIP can help government organizations (or other related organizations) to adhere to the new legal privacy framework constructed by the EU. The complexity of privacy, data collection and usage and information security will make it difficult for some government institutions to comply with these new standards, which only highlights the importance of the collaboration between relevant parties and the exchange of information and tools.

As this section has shown, the concept of awareness is used constantly when discussing privacy, data, and e-governments. Which seems to be legitimate, considering that the rapidity of technological developments is moving e-governments into unknown territory. So in a context in which local e-governments are forced to make use of these new technologies, the only thing that they can do is to evaluate every step methodically.

5.2 Transparency

E-governments have created a new situation that cannot be compared to any situation before in history. Never in history, there has been as much data collected as currently is happening. Based on my interviews, it is inescapable for governments to adapt and adopt towards these new forms of data collection and analysis. However, as governments collect and analyze more data, they also carry a stronger responsibility than ever before. These new values are also present in e-governments' transition to 2.0, especially in terms of transparency. When analyzing Utrecht's privacy regulation, the interviews and council meetings, it can be seen that the concept of transparency operates on multiple levels.

5.2.1 The transparency of data

In Utrecht's privacy regulation, much of the new laws and regulations are constructed for the sole purpose of transparency. Data should only be collected for a reason, and the reason for this collection must be available to the public. In addition, after anonymization and pseudo-anonymization, resourceful data should be given back to the public (Privacyverordening,

2016). This idea, Open Data, a familiar concept under the umbrella of e-government 2.0, is currently in operation in Utrecht (Gemeente Utrecht, 2017).

Besides providing information how data collection occurs, e-governments also have to maintain trustworthy to its citizens for allowing them to store these kinds of data. However, all of the respondents agreed on the notion that e-governments operate in a context in which 100% security will never exist. Schilderman states:

> "Systems at the moment are not as good, and I think they will never be as good that nothing can happen. So what you need then, is transparency. When things go right when they go wrong, and how they relate to each other. That is the level you need to be on, because perfect privacy and perfect systems, I do not believe in them'' (Interview 3, councilmember).

If perfect systems do not exist, new ways have to be found to maintain trustworthiness. Reuijl, argues that the only way to remain trustworthy as a government institution is to be transparent about privacy issues and report mistakes and wrongdoings to those involved. As mistakes are inevitable, the importance shifts towards what actions you take as e-government when mistakes occurred (Interview 6, director of CIP). This form of transparency is usually linked to the concept of data leaks, which came forward in all sources of information, from the interviews to the primary documents on the local, national and supranational level. In 2016, the e-government of Utrecht reported a public register including 22 data leaks, which shows that they are ahead of the new regulations of the GDPR that will be implemented on May 2018 (Gemeente Utrecht, 2016; EC, 2016).

Van Impelen argues that mistakes will be less likely if data minimization is the underlying principle in an expanding e-government. If you collect less data, there is also less data that can be leaked. Therefore, he is working on a new pilot in Utrecht to hand over data responsibility to citizens. The idea is that citizens of Utrecht will be able to log into a secure portal that will provide an overview in which departments of the e-government of Utrecht the individual is registered. Additionally, the individual citizen can request departments to remove their personal information from departments if Utrecht's e-government is not required by law to keep it (Interview 5, privacy officer).

Besides the transparency of the collection and loss of data, De Winter also sees an important role for transparency in terms of data usage. The newest data techniques such as big data and predictive behavior analytics are becoming increasingly interesting for all types of organization. If those techniques want to be used, transparency about these techniques are fundamental:

> "The most important thing when incorporating these new techniques is to keep the legal position of civilians and the democratic legitimacy in mind. In itself, there is nothing wrong to use these analytical techniques, as long as the individual can tell his own story. When predictions are made and acted upon, we really crossed enormous boundaries. The reality is, that you have no idea how you came to these predictions. Why did the computer think that? On what is it based? Which sources are used, and how are they weighed? How are the analysis executed? Without that kind of transparency, your conclusions could be entirely wrong" (Interview 3, IT-expert).

This means that in e-governments transition to e-government 2.0, the privacy of the government should not come before the privacy of individual citizens. Governments need to be willing to share their gathered data and analytical techniques in order to remain trustworthy. In this context, the best method to acquire this trustworthiness seems to be transparency.

5.3 Information security

Information security is one of the core dimensions of an e-government, which is primarily aimed at ensuring the functioning of digital services and information systems and the protection of data and privacy. According to Ruwhof, ethical hacker, it takes a lot of knowledge and time to stay up to date on the newest developments in information security. Within this dimension, he claims, it is possible to go from a perfectly protected digital government to a digital government that is as leaky as a sieve. Additionally, Ruwhof states that every year there are a few moments in which an organization or the Internet is vulnerable to breaches because official patches are either not released or not implemented fast enough (Interview 1, hacker).

According to De Winter, the largest problems in this dimension is the relationship between governments and the suppliers of information security software.

> "Local governments, such as Utrecht, receive low-quality software security packages that contain a lot of security implications. This is not only specific to government institutions per se, but is a more global problem. The lion share of the software that is made in the world is from a low-quality and contain common leaks. The information security industry is very immature, and specifically for local governments, you see that they are not able to obtain affordable software security packages" (Interview 3, IT-expert).

Ruwhof agrees with this notion. He says the only reason that local e-governments such as Utrecht are not breached by hacks from outside is that there is not a strong incentive for hackers to do a direct attack on these type of institutions. Only experienced hackers are able to pull off a specific directed attack, and the loot that is available at local e-governments are

simply not worth the effort (Interview 1, ethical hacker).

However, Ruwhof does argue that this is not only a problem that local e-governments are dealing with, because even the institutions that have most financial resources to spend on information security, such as banks and intelligence agencies, are able to be breached. The dimension of information security seems to operate in a context in which 100% security does not exist, and a balance has to be found between the possible damages and the level of information security that is affordable (Interview 1, ethical hacker).

6. Conclusion

The embracement of technology by governments is an inevitable result of all the technological developments that have occurred in the last decades. However, as government institutions are increasingly becoming more digital, we are only still beginning to understand the possible implications for informational privacy. Therefore, it is crucial to understand how privacy threats are evolving and how they can be protected in light of these profound technological developments.

In Utrecht's development towards e-government 2.0, privacy has obtained a more pivotal role in its process of digitalization. Utrecht's e-government is currently in the midst of the latest stages of Lee's (2010) stage model (morphing and e-Governance), in which the focus lies on refining old services and constructing new ones by means of modern technology. The progression made in terms of e-government also resulted in progress in terms of privacy maturity. It would be advantageous if future e-government stage models would integrate privacy maturity with e-government maturity.

In answer to the question how Utrecht's e-government design managed privacy whilst developing itself to one of the most digitalized local e-governments, two related concepts were identified: awareness and transparency.

Awareness embodies a certain state of mind in which in every aspect from e-government, implementations should be made consciously, with an understanding of their possible consequences for privacy. Utrecht's e-government is doing so by applying the core principals of privacy-by-design and privacy impact assessments. Privacy implications will be less likely when policy makers, employees, council members and operational managers are forced to consciously evaluate the consequences of data collection, storage, and usage. In addition, Utrecht also incorporated the core principle of data minimization, meaning that data will not be enriched or used if there is no specific necessity or acceptable justification for it.

There is a belief, among e-government practitioners in Utrecht as well as other

relevant actors, that privacy in this information age requires a basic underlying structure. The analysis has shown that government institutions are in need of a framework that sets certain standards, provides guidance on the complexity of privacy, and stimulates collaboration. By exchanging information and working together, privacy can be better protected without having to spend extra resources on it.

However, the analysis has also shown that complete security simply does not exist in the digital context e-governments operate in. As privacy implications and data leaks are inevitable, the best way to deal with this inevitability is to be transparent about when things go wrong. Transparency can be used to reduce citizens' privacy concerns and maintaining citizens' trust in local e-governments. The framework of Van Zoonen (2016) has shown that privacy concerns among citizens can be reduced if local e-governments only use impersonal or anonymized data for service purposes. So it will be the task for local e-governments 2.0 to be transparent about which data is collected and for which reason, and to put their own privacy beyond that of individual citizens.

This does not mean that by incorporating transparency and awareness the privacy of citizens' in Utrecht is completely guaranteed. Based on my analysis, the largest threat to privacy in a local e-government lies within the dimension of information security. The experts in this field all claimed that the information security of municipalities is the weakest of all government institutions. The lack of financial funds and knowledge make it impossible for them to construct a security system that cannot be breached. However, these problems regarding information security are not exclusive for local municipalities, but are also present at national governments, large financial institutions, and intelligence agencies. As long as the digital security of local e-governments manage to maintain a basic level, and the data of local e-governments remain relatively unprofitable, the threats to actual security breaches will be low.

Overall, it is evident that the transition of Utrecht's e-government towards the 2.0 model has sparked up the importance of privacy. Further research is needed to investigate whether becoming more mature in terms of privacy is an inescapable result of the process towards e-government 2.0, or whether the rising focus on privacy within Utrecht's e-government is a special case due to independent activism and actions. More importantly, in this rapidly changing technological context, it is the task of citizens, institutions, governments, and academics to constantly re-examine the core values of privacy. After all, privacy is one of our fundamental human rights and gives concepts such as autonomy, justice, community, and democracy the meaning that they have today.

7. Literature

Bannister, F. (2005). The panoptic state: Privacy, surveillance and the balance of risk. *Information Polity*, 10(1, 2), (p. 65-78).

Basu, S. (2004). E- government and developing countries: an overview. *International Review of Law, Computers & Technology*, *18*(1), (p. 109-132).

Boersma, K., Meijer, A., & Wagenaar, P. (2009). Unraveling and understanding the e-government hype. *ICTs, Citizens & Governance*: After the hype, (p. 256-66).

Bozeman, B., & Bretschneider, S. (1986). Public management information systems: Theory and prescription. *Public administration review*, (p. 475-487).

Byrne, B. (2004). Qualitative interviewing. Researching society and culture, 2, (p. 179-192)

Cate, F. (2002) Principles for Protecting Privacy. *Cato Journal Spring/Summer 22* (p. 33–57)

Corbin, J., & Strauss, A. (2008). *Basics of qualitative research: Techniques and procedures for developing grounded theory.* Thousand Oaks, CA: Sage

Crawford, K., & Schultz, J. (2014). Big data and due process: Toward a framework to redress predictive privacy harms. *BCL Rev.*, *55*, 93.

Dencik, L., & Cable, J. (2017). The Advent of Surveillance Realism: Public Opinion and Activist Responses to the Snowden Leaks. *International Journal of Communication*, *11*, (p. 763-781).

European Commission (2016). *Protection of Personal Data*. Retrieved from: http://ec.europa.eu/justice/data-protection/

Evans, D., & Yen, D. C. (2005). E-government: An analysis for implementation: Framework for understanding cultural and social impact. *Government Information Quarterly*, *22*(3), (p. 354-373).

Fang, Z. (2002). E-government in digital era: concept, practice, and development. *International Journal of the Computer, the Internet and management*, *10*(2), (p. 1-22).

Feinberg, L. E. (2004). FOIA, federal information policy, and information availability in a post-9/11 world. *Government Information Quarterly*, 21, (p. 439−460).

Gritzalis, S. (2004). Enhancing web privacy and anonymity in the digital era. *Information Management & Computer Security*, 12(3), (p. 255-287).

Halchin, L. E. (2004). Electronic government: Government capability and terrorist resource. *Government Information Quarterly*, *21*(4), (p. 406-419).

Introna, L. & Pouloudi, A. Privacy in the information age: Stakeholders, interests, and values. *Journal of Business Ethics 22(1) (1999), (*p. 27–38).

Kim, G. H., Trimi, S., & Chung, J. H. (2014). Big-data applications in the government sector. *Communications of the ACM*, *57*(3), (p. 78-85).

Koers, M. (2017). De Privacy Baseline. *Centrum informatiebeveiliging en privacybescherming*. Versie 3.0.

Labuschagne, A. (2003). Qualitative research-airy fairy or fundamental?. *The qualitative report*, *8*(1), (p. 100-103).

Lee, J. (2010). 10year retrospect on stage models of e-Government: A qualitative meta-synthesis. *Government Information Quarterly*, *27*(3), (p. 220-230).

Neuman, L. W. (2002). *Social research methods: Qualitative and quantitative approaches*. Pearson Education (US).

Norris, D. F. (2010,). E-government... not e-governance... not e-democracy not now! Not ever?. *In Proceedings of the 4th International Conference on Theory and Practice of Electronic Governanc*e. ACM. (p. 339-346)

Nour, M. A., AbdelRahman, A. A., & Fadlalla, A. (2008). A context-based integrative framework for e-government initiatives. *Government Information Quarterly*, *25*(3), (p. 448-461).

OECD (2014) 'Recommendation of the council OECD on digital government. *In OECD E Government Studies*. OECD, Paris, 2014.

O'Reilly, T. (2009). *What is Web 2.0?* O'Reilly Media Publications, Chicago.

Gemeente Utrecht (2016). *Privacyverordening 2016*. Utrecht. Retrieved from: https://zoek.officielebekendmakingen.nl/gmb-2016-135657.html

Gemeente Utrecht (2016). *Register Datalekken 2016*. Utrecht. Retrieved from: https://www.utrecht.nl/fileadmin/uploads/documenten/bestuur-en-organisatie/Register datalekken.pdf

Gemeente Utrecht (2017). *Open Data*. Utrecht. Retrieved from: https://utrecht.dataplatform.nl/

Gemeente Utrecht (2017). *WistUdata: Publieksdienstverlening*. Utrecht. Retrieved from: https://utrecht.buurtmonitor.nl/

Gemeente Utrecht (2017). *Gemeenteraadsdocumenten.* Utrecht. Retrieved from: https://ibabsonline.eu/Kalender.aspx?site=Utrecht

Picazo-Vela, S., Gutiérrez-Martínez, I., & Luna-Reyes, L. F. (2012). Understanding risks, benefits, and strategic alternatives of social media applications in the public sector. *Government information quarterly*, 29(4), (p. 504-511).

Rapley, T. (2007). *Doing conversation, discourse and document analysis*. London: Sage

Roode, M. de. (2016). Privacy Enhancing Technologies. *Researchgate*

Schelin, S. H. (2003). E-Government: An overview. In G. David Garson (Ed.), Public information technology: *Policy and management issues*. Hershey, PA: Idea Group Publishing (p. 120−137).

Solove, D. J. (2004). *The digital person: Technology and privacy in the information age*. NYU Press.

Solove, D. J. (2007). I've got nothing to hide and other misunderstandings of privacy. *San Diego L. Rev.*, *44*, 745.

Sivarajah, U., Weerakkody, V., & Irani, Z. (2016). Opportunities and Challenges of Using Web 2.0 Technologies in Government. In *Conference on e-Business, e-Services and e-Society* (Springer International Publishing. (p. 594-606).

Strejcek, G., & Theil, M. (2003). Technology push, legislation pull? E-government in the European Union. *Decision Support Systems*, *34*(3), (p. 305-313).

Seltzer, W. (1998). Population statistics, the Holocaust, and the Nuremberg trials. *Population and Development Review*, (p. 511-552).

Sweat, J. (2000), "Privacy paradox: customers want control – and coupons", *Information Week*, Vol. 781, (p. 52-3).

United Nations Department of Economic and Social Affairs. (2016). *E-government survey 2016: E-government in support of sustainable development.* Retrieved from: http://workspace.unpan.org/sites/Internet/Documents/UNPAN96407.pdf

Veljković, N., Bogdanović-Dinić, S., & Stoimenov, L. (2012). Building e-government 2.0 A step forward in bringing government closer to citizens. *Journal of e-Government Studies and Best Practices*, 18.

Waldo, J., Lin, H., & Millet, L. (2007). *Engaging privacy and information technology in a digital age*. National Academies Press.

Westin, A. (1970). Privacy and freedom. 1967. *Atheneum, New York*.

Whitley, E. A. (2009). Informational privacy, consent and the "control" of personal data. *Information security technical report*, *14*(3), (p. 154-159).

Zoonen, L. van. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, *33*(3), (p. 472-480).

8. Appendix

8.1. Additional information on respondents

In this section, additional information on the respondents is provided. The respondents are categorized by number to make referencing easier:

1# - Sijmen Ruwhof, ethical hacker.
2# - Dimitri Gilissen, council member of Utrecht
3# - Suzanne Schilderman, council member of Utrecht
4# - Brenno de Winter, investigative journalist and IT-expert
5# - Hans van Impelen, privacy officer of Utrecht
6# - Ad Reuijl, director of CIP
7# - Marleen Haage, council member of Utrecht
8# - Frans Vrauwdeunt, privacy officer of GGN and board member of NGFG

8.1.1 Respondents related to non-profit organizations within field of privacy

The first respondent in this category is Frans Vrauwdeunt who is currently a security and privacy officer at the GGN, a bailiff organization. He is also a member of the board of the "Nederlands Genootschap van Functionarissen voor de Gegevensbescherming" (NGFG). This organization is aimed at providing useful information to members, best practices, increase the knowledge on how to protect and secure privacy rights, improve the tools to ensure privacy and so forth. The interview was held in Dutch, and was conducted at the location of GGN in Utrecht. There was no one else present besides me and the respondent.

The second respondent in this category is Ad Reuijl, the director of the organization Center of Information Security and Privacy Protection (CIP). This is a network organization that shares information on how to deal with privacy and security concerns, and is an organization that was created by joint efforts of the Belastingdienst, DUO, SVB and UWV. The interview was held in Dutch, and was conducted at the headquarters of CIP in Amsterdam. There was no one else present besides me and the respondent.

8.1.2 Respondents related to Utrecht's e-government

Three respondents were interviewed that were related to the construction of the privacy regulation of Utrecht's e-government: Suzanne Schilderman (D66), Dimitri Gilissen (VVD) and Marleen Haage (PVDA). These three respondents are members of the council of the municipality of Utrecht, and besides their official function they all have personal interest on privacy, technology and the digital government. All the three interviews were held at the municipality building in Utrecht, and were all held in Dutch. The interviews were held seperately, and always in a one-on-one context.

Besides three council members, the privacy and security officer of the municipality of Utrecht, Hans van Impelen, has also been interviewed. This respondent is responsible for evaluating privacy policies within the various departments of Utrecht's e-government, and his task is to let Utrecht's e-government stay up to date with regard to privacy enhancing techniques. When new digital services are implemented, the performed Privacy Impact Assessments (PIA's) have to be approved by him. The interview was held in Dutch, and was conducted at the municipality building in Utrecht. There was no one else present besides me and the respondent.

8.1.3 Respondents that are active in the field of information security

Sijmen Ruwhof was interviewed, an ethical hacker who has executed several information security projects for large banks, local e-governments and private corporations in the Netherlands. On the 31st of January 2016 he made a post on his blog in which he gave a detailed description on how he hacked the Dutch elections. He was interviewed in order to obtain insight on the information security implications that e-government 2.0 might bring. The interview was held via the phone, and was conducted in Dutch. There was no one else present during the interview.

The second respondent in this category is Brenno de Winter, a respected reporter in the field of technology, privacy, and security. He successfully managed to show the Dutch government that the security of the digital government was inadequate by hacking the OV-chip card, resulting in national unrest. He was also one of the main reasons that the law 'Wet Openbaarheid van Bestuur' was created, which offers every citizen to have the possibility to request and inspect information that is in the hands of the government. This led to the Dutch government having a much more transparent approach Dutch government towards its citizens. The interview was done via phone, and was conducted in Dutch. There was no one else present during the interview.