From the Social Production of Indifference to the Digital Production of Invisibility

Experiencing the digitalization of bureaucracy in the Netherlands through the DigiD interface

Master Thesis
Cultural Anthropology: Sustainable Citizenship

Student: Vénicia Sananès

Student number: 2753863

Supervisor: Dr. Tessa Diphoorn

Word count: 21,624 words (excluding bibliography and appendices)

August 2021

Utrecht University

Acknowledgments

If this thesis is a success, I dedicate it to my supervisor Dr. Tessa Diphoorn best known as “Best MA Teacher of The Year 2020-2021”. It is your marvelous guidance, enthusiasm, and endless encouragements that enabled me to sharpen my thinking and bring my work to a higher level. As a thank you, I made sure you will not find any double-space in this thesis. I know how much this means to you.

I would like to express my gratitude to each and every participant who made this research possible. Thank you for sharing your time with me and trusting me with your experiences. I hope I did not fail you.

I am extremely grateful for my beau Sebastiaan who supported me with love, patience, and empathy, but mostly with food. Thank you for always putting up with me, even when I don’t deserve you.

With this very impersonal formulation, I thank all my friends for their unlimited support, compassion, and confidence boosts. I am sure you will understand that I have a word count to stick to.

I would also like to have a few words of acknowledgement for the greatness of Carolina Mills. The best friend and proofreader I could ever have imagined having.

But if this thesis is not a success, I dedicate it to my neighbors who will keep drilling, hammering and sawing long after this thesis.

Table of Contents

Introduction

A waiting room. What an uncanny place to be. This is what I think as I sit in the waiting room of the social center of Flevopoort, in Amsterdam East. I am about to interview a social counselor who helps people dealing with their administrative matters. I cannot remember the last time I had to go to a remote and unfamiliar building and wait for my turn to come. I have been living in the Netherlands for three years and I have only been once – the week of my arrival – to a public services counter. So who are all these strangers carrying a bunch of paper and why are they here? It is as if I have gone back in time. I remember when I used to sit in one of these impersonal grey rooms in France surrounded by strangers. There is something odd about how we start behaving as soon as we enter one of these rooms. Whether we decide to mark our entrance with a shy greeting or not, we all try to find a chair as fast, and especially as far from the rest, as possible. Once we have found our spot, we can start peeping and wondering. The only rule is to never catch their eyes. As we look back and forth between our feet and theirs, we try to decode every single detail about the way they look to guess the way they have come. But what is particularly uncanny about waiting rooms like this one is the bizarre tension between looking indifferent and being concerned. And this is when it hits me. We live in bubbles. Or anthropologically speaking, in contexts. On entering this room, my bubble has burst. I do not see strangers anymore. I usually sit on my couch, open my laptop and log in with my DigiD – a form of digital identification – to Dutch governmental websites and fill in digital forms. I do not bother collecting and looking for papers anymore, as they are stored somewhere on my computer, or in a "cloud". And if I really do need help, I hang on the line of one of those call-centers as I go on with my own business. This waiting room suddenly appears like a relic of a traditional bureaucracy full of strangers that we do not even see anymore.

DigiD stands for "digital identity" and is an identity management platform that allows government agencies to verify the identity of the users who are logging in to their websites. Each Dutch resident is strongly recommended to ask for a DigiD, which takes the form of a username and password. With this login code, Dutch residents can enter Dutch government websites and manage their administration online from the comfort of their couch, in an autonomous way. When I arrived in the Netherlands, I was at first impressed by the efficiency of the administration, so much so that my personal experience of DigiD has prompted this research. Furthermore, this large-scale digitalization of public services is not bound to the

Netherlands. Due to perceived bureaucratic dysfunctions, governments worldwide intend to improve their delivery and governance by digitalizing their public services (Fountain 2001) and are often referred to as "e-governments". However, in this thesis I prefer the term of "digital bureaucracy" to refer to this digitalization process of bureaucracy, and thereby approach DigiD as a digital form of bureaucracy. In doing so, I wish to look at this digitalization project from an anthropological perspective, to which bureaucracy has become a dominant field. In addition, the term "e-government" leads us to believe that digitalization processes have constituted brand-new governments, to such an extent that celebrants of digital technologies have come to argue that the traditional bureaucracy's hierarchical governance have collapsed (see Daniel Kreiss and al. 2011). Yet, as we can see from the above vignette, waiting rooms still exist. The Dutch bureaucracy did not cease to exist as soon as its services went online. In fact, waiting rooms have been displaced from official buildings of governmental institutions to social centers scattered throughout the cities. Because I do not see strangers seeking help in their communication with the government, it does not mean that these strangers do not need support, or worse, do not even exist. If DigiD facilitates my communication with the Dutch government, can we say the same for those strangers waiting in the social center of Flevopoort?

Through the understanding of the Dutch residents' experiences of DigiD, this thesis aims to understand whether this digital form of bureaucracy faces the same issues as "non-digital" forms of bureaucracy do. In other words, to what extent DigiD, as a digital form of bureaucracy, is different from "traditional" bureaucracies? As I situate this research within the anthropological debate on bureaucracy, I draw on Herzfeld's concept (1992) of "social production of indifference" and argue that DigiD is the *digital production of invisibility*.

Settling into the debate of bureaucracy

Bureaucracy has become a broad field of interest within anthropology over the past decade. Bureaucracy literally translates into a form of government that is predicated upon a desk, or an office. The theme of governance has produced the largest corpus of writing on bureaucracies in which anthropologists extensively describe how bureaucratic encounters shape and reproduce certain dynamics between states and citizens.

Michael Herzfeld (1992, 1) frames this relation between state and citizens as one of indifference, namely "the rejection of common humanity (…) the denial of identity, of selfhood". The state bureaucracy is the "social production of indifference" as it transforms

people into "humorless automatons as soon as they are placed behind a desk" (Herzfeld 1992, 1). This indifference, so he argues, creates sharp boundaries between "insiders" and "outsiders" (ibid., 26). Outsiders lose their identity and become "non-humans" (ibid., 26) as soon as they do not match the bureaucrats' little boxes.

Other anthropologists (Gupta 2012, Graeber 2015) show how bureaucracies are organizational and institutional structures that, once unfolded, reflect the structural violence of the societies in which and through which they operate. Overall, these studies tend to demonstrate how bureaucratic structure serves to reproduce the state and its inherent pre-existing inequalities.

However, the increasing digitalization of all aspects of life generates the formation and emergence of "new bureaucratic worlds" as Nayanika Mathur (2017, 4) posits. Whether governments adopt identity management systems like DigiD, smart ID cards like in Estonia, or biometric registration systems like in India, digital bureaucracies are mushrooming all over the world. Yet, anthropologists have only just started to join this debate on the digitalization of bureaucracy, mainly through the topic of biometrics technologies (Maguire 2009, Rao 2013, Hobbis and Hobbis 2017). On the whole, the anthropological approach of biometrics technologies primarily disputes the assumed neutrality of technology. For instance, Ursula Rao (2013) shows that, although the biometric registration implemented by the Indian government in 2009 is supposed to promote social justice and inclusive growth by rendering bodies legible in the systems of the state, it actually increases marginalization. Indeed, if biometrics promises "the recognizing of humans on the basis of intrinsic physical or behavioral traits", Rao (2013, 74) shows that while established and documented citizens are "easily absorbed into the new bureaucratic system", marginalized people like the homeless community remain excluded as their mutilated, scarred and dusty fingerprints are unrecognized - or unrecognizable - by "a system that posits healthy, young bodies as the norm". Rao (2013, 71) finally argues that the Indian biometric registration system fails to deliver on its promise of making a "currently invisible population visible to the welfare state". This biometric technology does not verify nor confirm the identity of vulnerable people, but rather shapes it. In this thesis, I similarly refute this technological neutrality. I primarily argue that class distinction remains, indeed, the most crucial structuring device, making of DigiD a class affair.

Rao (2013, 72) further argues that India's biometric project, as a "new effort to enhance the state's ability to direct populations through personalized support and surveillance" can be seen as a form of "governmentality" (Foucault 1991). Indeed, Michel Foucault's (1991) famous concept of "governmentality" refers to techniques and procedures for directing human

behaviors. It constitutes a modern form of power built on a type of regulated freedom that encourages individuals with what they are and what they could or should be, hence the semantic "the governing of mentalities". Foucault (1991) understands this new form of governing as the resulting effect of neoliberalism in modern societies in which "the market becomes the organizing principle of society, acting as an effective mechanism for regulating the extent, purpose, and reach of government" (Fraser 2020, 441). From this perspective, neoliberalism is not just "a set of economic policies based on monetarism, deregulation, and privatization, but also a productive power" (Fraser 2020, 437) that possibly signaled the start of a new paradigm in the governance of societies and human beings. However, if individuals are to be "governed through their freedom", they have, at the same time, to "make their decisions about their self-conduct surrounded by a web of vocabularies, injunctions, promises, dire warnings and threats of intervention, organized increasingly around a proliferation of norms and normativities" (Rose 2006, 150). Therefore, governmentality also entails a certain degree of conformity and uniformity towards certain ideals and practices.

The concept of governmentality (Foucault 1991) is particularly used in the anthropology of the state, which has produced the largest body of work on bureaucracies. Indeed, this concept offers a horizontal analysis of the mechanisms of government in which the state is no longer regarded as the sole actor, but rather as part of an assemblage with non-state actors that were previously thought to be distinct, such as society and family. Governmentality involves a de-centralization of the state and de-governmentalization of the practices of the state, which create a multiplicity of ramifications.

In this thesis, I approach DigiD as a form of neoliberal governmentality. Indeed, the digitalization of bureaucracy is catalyzed by wider neoliberal policies that aim to reduce state intervention and "opening up new markets in public services" (Whitfield 2012, 65). Moreover, DigiD serves as a tool to autonomize and responsibilize Dutch residents in their way to handle their administration, which ultimately aims to enhance the Dutch government's efficiency. Yet, unlike biometric technologies, DigiD is a digital service that requires from Dutch residents a certain digital literacy. Therefore, ensuring the governing of digital inclusion of the Dutch population is crucial for the implementation of this new tool of governance. However, the governing of digital inclusion is de-governmentalized, shifting the role of the state in this project onto a multiplicity of non-state actors "that have in heterogeneous ways sought to regulate the lives of individuals" (Rose and Miller 2008, 27). In fact, I propose in this thesis a slightly different approach to the concept of "governmentality", which I use to shed light on the *invisibilization* of a state withdrawing and governing "at a distance" (Rose 1993, 292) and of a

part of the Dutch population that is unable to join the digitalization process nor to conform with normative ideals and practices of self-reliance.

In fact, new approaches to bureaucracy have come to question this concept of "governmentality" (Foucault 1991) that often portrays an image of a too-unified and coherent state working on automaton. By focusing on quotidian bureaucratic practices, anthropologists (Nuijten 2004, Gupta 2012, Rao 2013) move away from the machinery metaphor of the state – inherited from Weber's (1922) conceptualization of bureaucracy. Gupta and Sharma (2006, 11) argue that "what the state means to people is profoundly shaped through the routine and repetitive procedures of bureaucracies", which they refer to as "the banal practices of bureaucracies". Therefore, by also being critical of this concept of "governmentality" (Foucault 1991) that tends to make invisible those who are not fit to lead self-fulfilling lives of happiness, I wish to shed light on the contrasting experiences that Dutch residents can have of the digitalization of bureaucracy, and thereby show how DigiD differently comes to affect their representations of the state. In fact, I primarily approach DigiD as an interface. An interface that, on the one side, creates connection by allowing a part of Dutch residents to communicate easily and efficiently with government, and on the other side, creates, or at least reinforces, the disconnectedness between the state and more vulnerable people of the Dutch society, making them *invisible* – and perhaps even more vulnerable as their trust in the state is simultaneously being eroded.

Finally, the emergence of "new bureaucratic worlds" (Mathur 2017, 4) opens onto new problematics regarding their management of cybersecurity and protection of their citizens' data privacy. First, the digitalization of bureaucracy is both the result of, and the aspiration to a better neoliberal governance (Fountain 2001) that reconfigures the role of the state and individual responsibility. Yet, the responsibilization process of individuals does not stop at one's own managing of bureaucratic matters. In this scheme, the DigiD user " as prudent citizen is [also] to become an active agent in the provision of security" (Rose 1999, 166). In addition, the securing of DigiD's IT systems also follows neoliberal imperatives of "marketization, privatization, and outsourcing" (Rose 2000, 324) of security practices. However, the understanding and the governing of digital bureaucracies require a certain IT expertise detained by a small amount of the population, creating more opacity, "secrecy" (Weber 2019) rather than the intended and promoted transparency (Alshehri and Drew 2010, Dandurand 2019) of the government. Therefore, I aim to show that there is something *invisible* about the (in)security of digital bureaucracies because we just cannot see them.

Second, the digitalization of bureaucracy also raises news concerns for the data privacy of citizens. Issues of privacy have largely been covered by sociologists (for an overview, see Anthony, Castillo and Horne 2017) but remain rather understudied by anthropologists. Anthropological observations concerning privacy are indirectly conveyed through debates about shame, secrecy, gossip, social manners, witchcraft, family life, and stigmatization (HIV/AIDS). More attention to privacy is given by anthropologists when they reflect, as researchers, on their own ethical conduct regarding the confidentiality of their informants. However, anthropologists have extensively documented the importance of documents in the anthropology of bureaucracy (for an overview, see Hull 2012) and this is how I decide to anthropologically approach these questions of privacy.

For the anthropology of bureaucracy, "documents are not simply instruments of bureaucratic organizations, but rather are constitutive of bureaucratic rules, ideologies, knowledge, practices, subjectivities, objects, outcomes, and even the organizations themselves" (Hull 2012, 253). Thus, if the materiality of documents, and more particularly, of papers play a crucial role in the governing of states and their bureaucracies, what about digitalized documents? When documents and files become *invisible data*, what implications does that have for governance, but more importantly, for people? Anthropologists also show how documents are not only instruments of rationalization, but also powerful and symbolic vectors of affect (Herzfeld 1992). This attention to affect draws analysis to moments of encounter with documents that can provoke emotions such as shame or pity (Hull 2012, Cody 2009). In contrast, what does the invisibility of these documents generate? By drawing from the well-documented argument "I have nothing to hide, so I have nothing to fear" (Lyon 2001, Marx 2003, Viseu et al. 2004), I argue that DigiD generates the "social production of indifference" (Herzfeld 1992) towards privacy concerns. In this research, I am less concerned to know whether DigiD constitutes a real threat for Dutch residents' privacy – although we will see that sometimes it does – and more interested in understanding the effects that the digitalization of documents has for the Dutch residents' perceptions of privacy. Yet, I argue that the Dutch residents' indifference to privacy concerns is due to the *invisibility* that DigiD creates. Dutch residents lose sight of their own data, and only then, they become indifferent to questions of privacy.

This research intends to consolidate the anthropological bridge between "non-digital" bureaucracies and digital bureaucracies through the theme of invisibility. Resting on Herzfeld's concept of bureaucracy being the "social production of indifference", I argue that DigiD is the

digital production of invisibility. As I actualize Herzfeld's concept, I aim to show that DigiD, as a digital form of bureaucracy does face the same issues as "non-digital" bureaucracies, only some are exacerbated and some are new. Rather than an abrupt shift, the digitalization of bureaucracy must be understood as the continuum of traditional bureaucracy. Through a critical approach of the invisibility that constitutes DigiD as a digital bureaucracy, I wish to shed light on the emerging social effects of this new technology in the making, which has become for most of us all too familiar.

My research population and location

My research takes place in the Netherlands, where DigiD was implemented in 2005 and where most of DigiD users are. For practical reasons, most of my research participants live in the same city as me, Amsterdam. In addition, the digital world constitutes my second research location not only because of the COVID-19 lockdown that was in place during my fieldwork, but also because it allowed me to further understand the various experiences of DigiD users through Facebook groups, online fora, governmental websites, news articles, YouTube videos, and Twitter accounts. Moreover, DigiD, as a digital technology, inevitably calls for this focus on the digital world.

Although Dutch citizens living abroad can apply for a DigiD, I decided to limit the scope of my research to Dutch residents only. In this thesis, I am less concerned with the nationality, age, gender and race of my informants than with their socio-economic status. All my participants have lived in the Netherlands for at least three years (if not born here) and they all speak English. Throughout my fieldwork, I have been able to organize my informants into four distinct categories that encompass the different Dutch residents' experiences of DigiD:

1. *The DigiD makers.* Due to our use of the concept of governmentality, one could argue that any self-reliant Dutch resident could be part of this category, each individual being a member of a community constituting a new ramification. Yet, I decided to narrow down this category to two different actors. The first being Logius, the management organization of DigiD that provide the entire infrastructure of this service. Second, librarians who ensure the implementation of DigiD at the local level by offering digital courses to Dutch residents who lack digital skills.
2. *The wealthy and/or educated users.* Most of my informants fall into this category, including the DigiD makers. However, this category focuses more on their experiences

as DigiD users. Their nationality, gender, race and age may vary however, they all are relatively digitally included, have had access to education and are between middle and high-class.

3. *The invisibles of DigiD.* This category does not refer to a homogenous group but comprises a diverse range of people in terms of age, race, or life trajectories. What they all share is a particular socio-economic position, one that makes them invisible to the rest of our informants and to DigiD itself. This category also includes the different people who help these vulnerable people using their DigiD.
4. *The experts.* This group refers to a group of informants I constituted on a forum called security.nl where users address all kinds of IT-related issues. These informants chose to remain anonymous, including to me. They are more digitally skilled than I will ever be, or in other words, they are who some might call "geeks".

My research methods and positionality

Anthropology is all about context. This statement never felt so true to me. I spent two months of my fieldwork on the "shiny side" of DigiD, interviewing DigiD makers and wealthy and/or educated users. It was only toward the end of my fieldwork that I discovered the invisibles of DigiD and that, eventually, I experienced what O'Reilly (2012, 24) calls the "iterative-inductive" approach. I was only blind from what I could not see, but with some time and an open mind, I finally broke free of my preconceptions. Indeed, my own experience of DigiD steered me in the direction to account for the easiness, accessibility and efficiency of DigiD. The invisibility of vulnerable users was reinforced by my own social background, as a twenty-one year old French student living in the capital of the Netherlands. Moreover, the coronavirus lockdown made it impossible for me to carry out participant observation across the city and perhaps to *see* these vulnerable users, or at least, more than this once in the waiting room I described earlier. Most of my fieldwork was "computer-mediated", therefore rendering those who are not digitally literate even more invisible. Yet, even when I discovered the existence of these vulnerable users through a documentary published online shedding light on their experiences of DigiD, it still was difficult for me to access the invisibles of DigiD. First, most of the invisible users do not speak English, or at least, not enough to be able to be interviewed for one hour on the topic of DigiD. I really experienced a language barrier during this fieldwork, even with some of the wealthy and/or educated users, and tried to create surveys in Dutch but I chose not to use them as they were poorly constituted. I do not think they could reflect all the

nuances that one's experiences consist of. Second, it was quite uncomfortable to reach out to invisible users who, as we will see, are busy enough with their problems, especially in times of a pandemic. Eventually, I gained access to these invisible users through "key participants" (O'Reilly 2012, 45), those who are helping the invisibles. Without the help of these participants, I would never have been able to understand the experiences and perceptions of the invisibles. Their participation was even more precious as they did not have a lot of time to grant me. In fact, one of them even was, as O'Reilly (2012, 46) puts it, my "gatekeeper". This participant directly put me in contact with an invisible of DigiD who was, in fact, the only person I was able to meet during this entire research. Therefore, seeing DigiD as an interface, I decided to create two very distinctive, or should I say contextual, chapters to actually mimic the proceedings of my fieldwork. As a matter of fact, the DigiD makers or wealthy and/or educated users will never meet with the invisibles of DigiD, and this is what I am trying to show also through the structure of this thesis.

Out of the nineteen semi-structured interviews, ten were face-to-face, eight were by video-call, and one by telephone call. I also carried out a focus group discussion with nine of my friends on the theme of privacy, face-to-face. However, most of my fieldwork was computer-mediated and like Christine Hine (2020, 4) notices I could not help but "be affected by the general cultural current of concern that mediated communications might not be quite as good as the real thing", especially when the precious words of my informants were scattered by a poor Wi-Fi connection. Doing fieldwork during a pandemic also reinforced somehow the artificiality of the relationships with my research participants. Although our task as ethnographers is to create solid and honest relationships with our informants, it is not always easy to build that trust and sincere interest through a computer window and a timer counting the remaining seconds of our conversation. Let alone the disappointment of not *being in the field* and surrounded by more and more people every day. Yet, I do not feel like my findings have negatively been impacted by this pandemic. I was still able to understand the various DigiD experiences of Dutch residents. I also was able to go off-line in order to reach out to the invisibles of DigiD, and I hope this thesis will fairly reflect their experiences too. Inversely, I would never have met with the experts if I had not spent so much time behind my computer, looking for new sources of information.

Because I was unable to carry out participant observation, next to interviewing, I mainly focused on doing online observation of Twitter, Facebook group, fora and comment sections of the DigiD app – which offers users another way of to log in - on the Google Play Store and Apple Store. Furthermore, extensive textual analysis of official brochures on the theme of

digital inclusion or digitalization, governmental websites and news articles enabled me to understand the rationale and the official rhetoric of DigiD.

Although this thesis is about what I have been able to do, you should know that I also experienced red tape while studying this digital bureaucracy. Except with most of the wealthy and/or educated that I knew beforehand, them being friends or friends of friends, I always made the first contact via email, most of which remained unanswered. For instance, when I tried to get in touch with the DigiD makers in charge of the DigiD's Twitter account, I spent weeks sending emails and calling employees who would keep repeating to me "I will forward your request to my colleague, and someone will call you back". After innumerable attempts, I eventually accepted this refusal, or perhaps indifference, as being part of this digital and invisible bureaucracy, which eventually led me to the findings that I am presenting you with today.

Outline

In this research, I primarily argue that DigiD is the digital production of invisibility. My argument is three-fold and follows the outline of this thesis.

The first chapter portrays the first side of the DigiD interface. After explaining the origin and rationale behind DigiD, we will see how DigiD is primarily experienced by wealthy and/or educated users as a tool that facilitates their communication with the government. We will then approach DigiD as a form of governmentality that, on the one side, governs – via the help of the DigiD makers – the digital inclusion project, and on the other, engineers the invisibilization of the state, which Dutch residents are sometimes critical of.

We will then shift to the other side of the DigiD interface through the experiences of the invisible users. I aim to show that DigiD – as a digital form of bureaucracy – not only continues to exclude the same vulnerable people of society but reinforces bureaucracy itself, especially for these vulnerable users who end up becoming more dependent rather than self-reliant. Yet, we will see that DigiD renders vulnerable people invisible, both to the state and to the digital inclusion strategies.

In the last chapter, we will see how the invisibility of DigiD obscures issues of (in)security to the large majority of the Dutch population. We will observe that DigiD users do not even have the necessary knowledge to govern their own security, even though they are required to. Based on Dutch resident's perceptions of privacy, we will understand that their indifference is generated by the invisibility that DigiD creates.

Chapter 1: The Lustrous Machinery of DigiD

Introduction

In this chapter, we will exclusively focus on the DigiD makers and on the experiences of wealthy and/or educated DigiD users. After retracing the creation of DigiD and understanding its functioning from the DigiD makers' perspective, we will see that this new technology is a neoliberal form of governmentality that perfectly fits the market mentality while empowering all the actors of this machinery. Ultimately, we will examine how the invisibilization of the state ultimately impacts Dutch residents' experiences of DigiD as well as their perceptions of the state.

The rationale behind DigiD

Think of DigiD as a digital proof of identity. Whenever people go to the City Hall or to the counter of a different government institution, they usually start by showing their ID card, passport, or driving license. In the Netherlands, residents can log in to government websites with their DigiD and prove their identity. It consists of a username and password that users can choose themselves. Each DigiD is linked to one's unique citizen service number (BSN, from the Dutch: *Burgerservicenummer*). This unique citizen service number is issued after Dutch residents have registered in the Personal Records Database (BRP, from the Dutch: *Basisregistratie Personen*) of the Netherlands. Everybody living in the Netherlands for longer than four months must register as a resident in the BRP.

DigiD originated in 2003 when the Dutch government launched the "New Authentication Facility" (in Dutch: *Nieuwe Authenticatie Voorziening*), most commonly known as *Burgerpin*. In 2004, the name was changed to DigiD. It was set up by a foundation called ICTU (in Dutch: ICT- Uitvoeringsorganisatie – which literally means: "implementation organization of information and communications technology"). ICTU was created in 2001 by the Ministry of the Interior and Kingdom Relations to support and facilitate government organizations in the development, introduction and implementation of ICT. As stated on the ICTU's website,[1] "as an independent consultant and executor within the government", ICTU works "from the conviction that ICT helps the government move forward with social issues".

[1] "About us," ICTU, accessed July 29, 2021, https://www.ictu.nl/about-us.

At the beginning, DigiD only started for the municipalities that wanted to offer their services to their residents digitally instead of at their counters. The reason for the implementation of DigiD was to outsource the authentication process of citizens. This way, municipalities would be able to concentrate on their core tasks, namely the delivery of their services, rather than setting up their own authentication software and dealing with all the citizens who would experience problems with their login credentials, or other IT-related issues. From there, DigiD would completely take care of this authentication process and provide assistance to users through its helpdesk (via telephone, email, and webcare).

Since 1 January 2004, Dutch residents have been able to digitally identify themselves not only with their municipalities, but with other government organizations. But how does this authentication process work in practice? Once a user is on the website of the organization he/she wants to communicate with, he/she is asked to connect with his/her DigiD. After the user is logged, he/she is automatically sent back to the original website. DigiD then communicates the unique citizen service number that is linked to the user's DigiD, which fully guarantees the identity of the user to the organization in question. This authentication process takes more words to explain than seconds to happen. In fact, if the login credentials are correct and the user is familiar with this system, it works flawlessly. In a few seconds, the user is recognized by first DigiD, then the organization and everybody then can go on with their business. Dutch residents do not stand in line with their identity papers waiting for someone to check them, nor do they need to click on innumerable links to go from the organization's website to the DigiD's website, and then back to the organization's website. This authentication process is therefore easy and instantaneous for users (see appendices A.1) and effortless, even though it is more complex from the organizations' perspective (see appendices A.2). When we look at the organizations' perspective, this authentication moment seems much more complicated – and bureaucratic – than the act of showing someone a passport. Although, now with DigiD it is for both government organizations and users invisible.

DigiD also offers users a choice between four login methods, which chronologically succeed one another, adding each time an extra layer of security:

1. With a username and password that users have previously created and therefore are more likely to remember
2. Since more and more organizations require a two factor-authentication (2FA) for security reasons, the SMS-check login method is the most used. After entering their username and

password, users receive a code by SMS (or by call) which they have to copy to be granted access.

3. In order to reduce the SMS costs, Logius created in 2017 the DigiD app, another 2FA system. Users do not need to remember their username and password, but only a self-chosen PIN code (four digits). This app is promoted by Logius[2] as being the "easiest way to log in securely".
4. Finally, since 11 January 2021, users can also log in with a recent Dutch ID card or passport that contains a chip that the NFC reader (the same technology that enables us to do contactless payments) of the smartphone can read through the DigiD app, adding again an extra layer of security.

As more and more government organizations have transferred their services online and offered authentication via DigiD, the Ministry of the Interior and Kingdom Relations decided in 2006 to create the GBO.Overheid – called Logius since January 2010. Logius is the government agency – part of the Ministry of the Interior and Kingdom Relations – that provides services and products for the digital government. Or as Logius itself puts it on its websites' homepage[3], "[Logius] work[s] at the heart of the digital government and [is] proud of that". But more importantly, Logius is the organization that now manages DigiD. Logius is responsible for, as written on its website[4], "the availability, correct operation, continuity, security, customer support and monitoring and further development of DigiD". In other words, Logius provides the infrastructure of DigiD and ensures its good functioning for both users and *customers*. In fact, DigiD transforms both users and organizations into customers. Users become customers of the organization on which they are logging in, and organizations become customers of Logius. Under the "Benefits" section of its website, Logius writes:[5]

> DigiD is practical for you as an organization and for your customer. For example, with DigiD, you can speed up your registration procedure or increase convenience for your users. This will give you a higher customer satisfaction.

[2] "Log in to my DigiD,"DigiD, accessed July 29, 2021, https://digid.nl/inloggen.
[3] "Homepage," Logius, accessed July 29, 2021, https://www.logius.nl.
[4] "DigiD: who does that," Logius, accessed July 29, 2021, https://www.logius.nl/diensten/digid/wie-doet-wat.
[5] "Services: DigiD," Logius, accessed July 29, 2021, https://www.logius.nl/diensten/digid.

Let's recall here that DigiD was created by the ICTU foundation, thereby a non-profit organization, and was only used by a few municipalities. Today, Logius sells DigiD, as an authentication service, to 642 organizations.[6] In 2006, Logius counted 3,5 million authentications with DigiD that each costed 3,5 euros, excluding VAT.[7] In 2020, Logius registered 402,5 million authentications with DigiD that each cost 0,138 euros, excluding VAT.[8] As the number of authentications rose, their price went down. The more organizations use DigiD, the more Logius can absorb the costs of this service and therefore reduce its price (see appendices B). However, in 2017, the Council of Ministers decided that "from 1 January 2018, all costs for the management and operation of DigiD will be passed on to customers. This financing agreement is intended to keep the digital government safe, usable and future-proof".[9] This decision shows how the state further withdraws from its role in the provision of public services, as it now charges organizations for all the costs of the DigiD authentication service. In fact, Logius modifies the rates of DigiD every year as if DigiD– or at least, the delivery of public services – was a fluctuating market. Although I am unable to provide a deeper analysis of these numbers (see appendices B), it becomes clear that Logius is *not* a non-profit based organization. Moreover, Logius also offers DigiD to private organizations such as insurance companies and saw an increase of 10 percent in its budget of 2020 (223 million euros) compared to 2019. This budget rise is explained by "an expected increase of staff, both internal and external".[10] Logius itself outsources its needs for ever increasing IT equipment and expertise. To put it simply, DigiD is perfectly tailored to the market mentality.

However, for informant Jeroen, a representative from Logius, "DigiD is such a big success" because it rests on a strong historical legacy. During our interview, he narrated how, to understand this success, we need to go back to Lucien Bonaparte – Napoleon Bonaparte's brother. In 1801, Lucien Bonaparte and Jean-Antoine Chaptal organized the largest French population census, which started a series of censuses carried out every five years until 1946. Although population censuses have been carried out for five thousand years by China, Egypt,

---

[6] "Which organizations participates," DigiD, accessed July 29, 2021, https://www.digid.nl/en/wat-is-digid/wie-doen-mee/.
[7] "Logius Annual Report 01," Logius, accessed July 29, 2021, https://magazines.logius.nl/logiusjaarverslag/2017/01/financien.
[8] "Invoicing and Rates," Logius, accessed July 29, 2021, https://www.logius.nl/onze-organisatie/zakendoen-met-logius/doorbelasting#:~:text=DigiD%3A%2012%2C1%20cent%20per,btw%20(netto%2Dtarief).
[9] "Invoicing and Rates," Logius, accessed July 29, 2021, https://www.logius.nl/onze-organisatie/zakendoen-met-logius/doorbelasting#:~:text=DigiD%3A%2012%2C1%20cent%20per,btw%20(netto%2Dtarief).
[10] "Logius Annual Plan 2020," Logius, accessed July 29, 2021, https://programmeringsraadlogius.pleio.nl/file/download/3210053a-4af3-4d19-a768-d2c2aa87f05e/1581409934bijlage%207a%20jaarplan%20logius%202020%20-%20definitief.pdf.

the Roman, and Inca Empires, Lucien Bonaparte and Jean-Antoine Chaptal achieved the first exhaustive census of the modern era through ninety-eight departments and succeeded in registering more than thirty-three million inhabitants. Jeroen qualifies the 1801 census as "the base of the population registration". As previously noted, every Dutch resident is registered in a central database, which renders the implementation of a system like DigiD much easier. Lyon and Bennett (2013, 17) indeed argue that "all identification systems must be built upon the pre-existing legacies of past policies". Therefore, identification systems like DigiD are technologies through which nation-states can consolidate their previous unification projects. With more than 18,3 million accounts in 2020,[11] DigiD has rapidly penetrated the Dutch society that counts 17,5 million inhabitants – and this is why Jeroen thinks DigiD is "such a big success". If there are more accounts than inhabitants in the Netherlands, it is because former Dutch residents living abroad can also apply for a DigiD and because inactive accounts, of deceased people for instance, are only deleted three years after the last login.

"It's just one gate to all these areas of your life"

After a few interviews, I was actually surprised to notice that first, there was a certain homogeneity in the definitions of DigiD given by my research participants and that this matched the official one, which I drew from several textual analysis – namely, DigiD is easy, accessible, and efficient. In this section, I want to show how DigiD is primarily experienced as being easy, efficient and accessible, and how this is due to one's socio-economic position and digital inclination. For my informants, DigiD often generated words such as "key", "door", "gateway", "access point", and "tool". At the beginning of my fieldwork, I felt like DigiD was so common and easy for my informants that they did not always understand the point of my research, and especially of these interviews. In fact, it is because DigiD, as a form of governmentality, has become so familiar to my participants that it was maybe more difficult to talk about it and to reflect on it. In this section, I want to show how DigiD is primarily experienced as being easy, efficient and accessible, and this is due to one's socio-economic position and digital inclination.

Let's take Heleen as an example. Heleen is a wealthy stay-at-home mother of two who finds DigiD very handy. "For me, it is just an easy way to get in my information, to get to the

[11] "Logius Annual Report 2020," Logius, accessed July 29, 2021, https://magazines.logius.nl/logiusjaarverslag/2020/01/4-logius-diensten-het-jaar-in-cijfers.

local government, or to see my driving license", she says. Heleen can handle all the administrative tasks for her family, in an autonomous way, from her computer. She is the bureaucrat of the house. Also, she never had to contact the DigiD helpdesk or ever even experienced any problem with one of her family member's DigiD. Like most of my research participants, Heleen only uses DigiD a few times a year "for very simple things such as a passport or the school" of her children, which consequently shapes her perceptions of DigiD. Wealthy users like Heleen do not need to apply for benefits or look for a job via the Employee insurance Agency (in Dutch: *Uitvoeringsinstituut Werknemersverzekeringen* or UWV), which both require to log in via DigiD. Most of my informants mainly use DigiD to submit their annual income tax return on the website of the Tax Office (in Dutch: *Belastingdienst*). In 2006, DigiD became mandatory for everyone who wants to fill an income tax return digitally. Like Heleen, most of my informants submit their tax return digitally thanks to their DigiD as it takes about ten minutes to check the already pre-filled information and to submit it. In other words, she adds, "it works for me".

Mariska is a young Fashion Design student that lives in the city center of Amsterdam. When she moved out from her parent's house, she started to use her DigiD herself. When I ask her how she feels about this, she explains:

> Somehow it feels so grown up that you have to sort things out yourself but I think that on the computer with DigiD everything is so clear that nothing can go wrong actually, and that's making me feel good.

Mariska feels very comfortable with technology. And because DigiD is "*gemakelijk*" which she translates as "easy to access and user-friendly", it takes away some of the anxiety that can come with doing administrative tasks. In fact, she kind of experiences DigiD as a *rite of passage* into adulthood, where she now has to deal "with very serious things". However, the user-friendliness of the DigiD interface smoothly guides Mariska into becoming an autonomous and responsible individual. To such an extent, that she also becomes, in a way, critical of DigiD. For instance, she stopped using the DigiD app because she says that she "expected more" of it. She thought that the app would be, like DigiD promised users, "easier".[12] Although she understands that a two-factor authentication is required for security reasons, she finds it "a bit annoying to have a

[12] "Login methods," DigiD, accessed July 29, 2021, https://www.digid.nl/en/login-methods.

second login". Although we will dive deeper into these questions of security in the third chapter, it is interesting to notice how users progressively become clients, each one carrying expectations and providing feedback. At times, during interviews, I felt like my informants were seeing me as a representative of DigiD, or at least, as if they were hoping that I would pass on their comments to DigiD itself, or even more relevantly, as if they did not have anyone else to listen to their feedback. But this is even more striking if we browse through the thousands of comments that users have written for the DigiD app in the Apple Store or Google Play Store. Like for any other app, users can choose to leave a review and give a rating between one (as the minimum set by the app store) and five stars. The DigiD app achieves a score of 4.3 out of 5 both in the Apple Store and the Google Play Store, based on respectively 246 000 and 87 916 comments. Thus, most of the users provide positive feedback like in this five-stars review from the Apple Store:

> Super handy. We can't make it any easier. Nice secure app. (From the Dutch: *Super handig. Makkelijker kunnen we het niet maken. Mooie veilige app*)

Yet, some users are more critical due to upset whenever the DigiD app does not work for them, as we can see on this comment from the Apple store:

> I did not want to put any star, but since one seems to be the minimum… I receive on DigiD a useless message saying that the screen was not used for 15 minutes. Using another browser did not work, even removing and reinstalling the DigiD app did not work. It seems like the Dutch government again are not able to create a working system. Obviously helpdesks are not reachable ☹ Even this review appears to be difficult to post as all nicknames are taken….

Therefore, do these reviews demonstrate a certain shift in the attitude of Dutch residents vis-à-vis the Dutch bureaucracy as they embody a more customer-oriented mentality? Or are these comments a way for helpless users to make themselves heard and seen? It seems, that depending on one's experiences of DigiD, it is a bit of both. One thing is clear though: DigiD allows the Dutch government to take a step back so nothing stands between organizations and users, except sometimes, a heartless and unresponsive screen.

The governing of digital inclusion

During interviews, I asked my participants their average screen time per day. After a dozen interviews, I realized that there was a correlation between one's experience of technology and one's perceptions of DigiD. The more comfortable the user is with digital technologies such as smartphones, computers, or tablets, the more positive his/her experience of DigiD is. And this is exactly the conviction of the Stichting Digisterker, which literally means "the foundation that makes you stronger digitally".

Piet is the founder of Stichting Digisterker. Digisterker is a foundation that creates course materials on how to work digitally with the government and sells them to libraries or schools. During our interview, Piet explains the conviction on which stands his foundation:

> The best incentive for making people use digital technologies is to develop their skills to such an extent that they become comfortable with them, self-confident, that they develop a trust in themselves that enables them to work independently and safely with the digital services of the government

Therefore Digisterker does not only support Dutch residents in the use of digital government services but also enables them to blossom and thrive in society. By following the digitalization of the Dutch society and developing their own digital competencies, Dutch residents should not only be more digitally included but also maximize their happiness and freedom. This is why I approach DigiD as a form of governmentality. Digital inclusion is not only one of the strategies of this governmentality but also comes as a requirement. Those who already are digitally included, like Heleen or Mariska, easily embody DigiD whereas those who are not will just "have to get used to it" as Piet says because "this is the only way forward". In short, there is just one word between digital exclusion and digital inclusion: will – and Dutch residents must develop their digital competencies to become empowered subjects. On another note, enabling users to connect themselves with their DigiD also financially benefits organizations. Users can request a "DigiD authorization" (in Dutch: *Machtigen*) which gives the permission to someone else to arrange their administration online for them. However, I will just add that each

authentication with this option currently costs 0.88 euros against 0.13 euros for an autonomous authentication.[13]

As I mentioned in the introductory chapter, DigiD, as a form of governmentality, has various ramifications. Governmentality works like a machine: every piece is essential to the good functioning of that machine. So, although there is not one component more important than another, some do have a bigger task and this is the case of the librarians in the Netherlands.

"I like to give DigiD courses because that really helps people"

Han is in his forties and loves being a "specialist of the digital library", especially due to his teaching role. Indeed, Han is also a Digisterker teacher. To become a certified teacher of Digisterker, he had to take a small training program proposed by Piet's foundation. Han has been teaching Digisterker for ten years. In the beginning, he recalls, his public was diverse, "men and women, well mostly women" who were between forty and seventy years old. But for the last couple of years, Han has primarily been teaching to women above seventy. He describes his students as people who "don't have a computer, don't know exactly how it works, and want to know how to use DigiD, or how to use the Internet". A Digisterker course usually lasts eight hours, two hours per week during one month, at the end of which students should be digitally self-confident. Although it is quite an ambitious promise, Han assures us that his students always end up becoming more digitally self-confident because "that's one of the most important things of the lesson". He then adds, "I like to give courses because that really helps people".

Han is not the only one passionate about his role in this digital inclusion project. In fact, the two other librarians/teachers that I have interviewed communicate the same enthusiasm about giving these Digisterker courses. In a brochure published by the Digital Government in 2019,[14] it is stated that "around 2,5 millions Dutch people find it difficult to use digital devices" So, in order to bridge the digital divide, the role of local libraries has been intensified and even revalorized. When I ask Jacqueline, both a librarian and Digisterker teacher in her fifties how she feels about this new role, she says:

---

[13] "Invoicing and Rates", Logius, accessed July 29, 2021, https://www.logius.nl/onze-organisatie/zakendoen-met-logius/doorbelasting#:~:text=DigiD%3A%2012%2C1%20cent%20per,btw%20(netto%2Dtarief).

[14] "Digital inclusion: Everyone must be able to participate," Digital Government, accessed August 1, 2021, https://www.nldigitalgovernment.nl/wp-content/uploads/sites/11/2019/02/digital-inclusion-everyone-must-be-able-to-participate.pdf.

> Yes, yes. I'm very proud that… I work in the library world for 30 years but they did it really well, because we are now seen as a partner that can help you to find the correct information. Where to look for and how to find information. That is what I always say, I know where to find the right information. That is my job. In the old days, I presented you a book. But now I present you a website where you can find it. And I will show you that it's safe, and I will show you how you should use it to keep it safe. That's really my job. I'm really happy now that I am a Digisterker teacher and that I can do that in that way. Because that is really the basic of my work, how I started with this work. It's really important. I'm really happy, I'm really proud of the KB [*Koninklijke Bibliotheek* - the National Library of the Netherlands] that they have a good contact now with the *overheid* [government], that we can have that role again. I'm really proud of that.

To sum up, the digital inclusion project engineered by DigiD gives a role, or even a purpose, to everyone in society. Jacqueline and Han both find fulfillment in being part of such a happiness and freedom enterprise, which they really experience first-hand as they transform their students into self-confident individuals able to now thrive in society. And this is one of the main virtues of governmentality. It is not about tricking people into thinking a certain way, or into adopting a particular set of conducts and values. Freedom does not simply become a sham. Instead, it is about merging political projects with individuals' own projects for self-mastery. As Rose (1993, 298) puts it, "it is to say that the agonistic relation between liberty and government is an intrinsic part of what we have come to know as freedom". Therefore, we can better understand why Jacqueline's students gradually change their perception of DigiD and of the state as they follow her course:

> I always give four lessons. When they start the first lesson, they think they are forced. They don't want it, but they have to do it. I always start with a sheet of Digisterker about that and then I try to make the conversation – what do you think? Is it easy? Is it fast? No, no, no. And then I bring that sheet again on the last lesson and then they think – oh yeah! Oh this is convenient, this is convenient, yes, oh ja. It's good. So they change a little bit. But first, when they start there is a big NO. I don't want it, I'm forced, I don't want it, they force me. THEY. The government. They force me.

Ultimately, this is what governmentality is. By following these courses, even the most reluctant Dutch residents end up embracing DigiD. As they become their own subject, the state fades away. When I asked Mariska how she feels about the state, she answered: "well, it doesn't feel like a really big organization, even though I know it is". And this is what I call the *invisibilization* of the state. The state is not a big, centralizing, and over-reaching entity anymore. In fact, it reproduces itself into individuals, through the proliferation of multiple entities, "at a molecular level" (Rose 1993, 298).

In fact, libraries are not the only spaces for digital inclusion. As we can see from the pictures posted on the DigiD's Twitter account (see appendices C), family is one of them. Whether they show a grandfather being helped by his grandchild, or a father supported by his son, DigiD is staging an intimate digital inclusion moment. This transferability of skills between family members saves time and money to the government, and even seems enjoyable for family members themselves.

Furthermore, as we search for information about DigiD online, we stumble across dozens of non-governmental websites or blogs that explain more in detail what DigiD is and the application process. On YouTube, we can even find videos from newcomers who explain to future Dutch residents how DigiD works. I interviewed two of these YouTubers. Harshil[15] and Seb[16] both created a YouTube channel for expats and students coming to the Netherlands. Among other topics, they both edited a video on DigiD. Their video on DigiD is one of the most viewed videos on both their channels. They describe DigiD's application process as "one of the first things you have to do when you move to the Netherlands". Although they and their subscribers are digitally literate, they feel like there was a demand for that video. When they arrived, they found all these formalities a bit overwhelming, and wished they had a video about DigiD to guide them into their new life here, which – once again – both shows and generates the invisibilization of the state due to the governmentality machinery.

[15] "How to apply for a DigiD," Sparkle Together, YouTube, accessed July 29, 2021, https://www.youtube.com/watch?v=IwV7KCne4iU&ab_channel=SparkleTogether.
[16] "First week after moving here – Register for DigiD," Come To Rotterdam, YouTube, accessed July 29, 2021, https://www.youtube.com/watch?v=MTapqBfo8zY&t=155s&ab_channel=ComeToRotterdam.

When invisibilization feels like indifference

If all my informants take enjoyment from the autonomy that DigiD provides, they all share the same critique, being: government organizations are impossible to reach. Librarians all explain how their students, mostly older people, "really do miss human interaction. It is something [they] hear a lot". Regarding wealthy and/or educated users, most of them regret that "lack of assistance" when they rarely, yet sometimes do need it. As Jacqueline further explains:

> For instance, with the UWV [Employee Insurance Agency] it's terrible how you cannot find out how to call them. Really terrible. It's a disgrace, I must say. Because a lot of people are in a very vulnerable situation, it's about work, it's about money… I really think it's a disgrace. It's very difficult to find somebody. It's a disgrace that there is no human person to contact.

This invisibility allows the state to insulate itself from social suffering, as Herzfeld (1992) explains with his concept of "social production of indifference". In that sense, DigiD, as a digital bureaucracy, is not different from "non-digital" bureaucracies which Herzfeld (1992) described almost thirty-years ago. Although, today DigiD goes one step further as it almost suppresses any physical interaction. For example, it is almost not possible anymore for Dutch residents to go to the Tax Office and get help to fill in the tax return form. Or as one of my informants puts it, "in the Netherlands, they are very good at not making you go anywhere". Moreover, the call center of the DigiD helpdesk illustrates the continuity of a traditional bureaucratic system. Whenever users try to call DigiD, they have to press the number that corresponds to their question, wait – sometimes for a very long time – before being helped by an agent who is not allowed to access their personal information. The DigiD helpdesk only deals with IT-related issues or lost password, but not with personal administrative questions. Users are therefore sent back to the right administration, and another call center, and etcetera. It seems that DigiD just displaced the common bureaucratic maze into the digital space.

Conclusion

We have seen how DigiD - as a form of digital bureaucracy tailored to the neoliberal needs for decentralization, outsourcing, and competitiveness – is also a form of governmentality that shapes Dutch residents in their conduct and aspirations. By simultaneously impelling Dutch residents to be digitally included and de-governmentalizing the digital inclusion project through

various ramifications, DigiD generates the invisibilization of the state. This invisibilization of the state reproduces the same mechanisms of indifference that are inherent to bureaucracies.

However, governmentality forgets a small detail: the structuring and *stricturing* effects of social class. If my wealthy and/or educated informants find DigiD easy, efficient, and accessible, can we say the same for people from lower classes? In fact, DigiD – as a form of governmentality, and thereby as a process of uniformization – excludes those who do not fit within its ideals of self-mastery and self-fulfillment, pushing them outside of this machinery and rendering them invisible – especially to my wealthy and/or educated informants.

Chapter 2: The Invisibles of DigiD

Introduction

Seeing DigiD as an interface, this chapter focuses on the other side – namely, the *invisibles of DigiD*. In the previous chapter, I demonstrated how DigiD – as a form of governmentality – ultimately generates the invisibilization of the state. Yet, in this chapter I aim to show how this invisibilization also renders invisible those who do not – because cannot – fit within the values, ideals and principles of the DigiD's governmentality machinery. As the digital inclusion programs and strategies do not – because cannot – even reach the most vulnerable people of the Dutch society, DigiD disconnects from the state these Dutch residents from a lower socio-economic position. This digital form of bureaucracy is therefore no different from "non-digital" forms of bureaucracy as it reproduces the same pre-existing inequalities. Yet, this digital form of bureaucracy exacerbates these inequalities and reinforces bureaucracy itself as it renders those already excluded totally invisible, making them even more vulnerable. In this sense, DigiD is – once again – the *digital production of invisibility*.

The reinforcement of bureaucracy

> One more day behind my desk – or should I say, in my armchair – trying to understand other people's perceptions based on other people's work. When will I get to see people face-to-face, or at least, face mask-to-face mask? It is the 2nd of April 2021 and I am spiraling. Karen O'Reilly says that fieldwork is an iterative-inductive process, but I swear that mine starts feeling way more iterative than inductive. So, as I browse, surf, scroll and click, I finally stumble across something different. Something drastically different. It is a documentary called "DigiD is unsuitable for informal caregivers" [*DigiD ongeschikt voor mantelzorgers*]. My Google translator must be wrong because this truly feels like an oxymoron. Worse, this goes against everything I've been researching for the last two months. After I watched this documentary, I realized that these twenty-five minutes were probably the most important minutes of my research. Thanks Karen.

This vignette based on my fieldnotes relays the moment I discovered the invisibles of DigiD. This documentary[17] from NPO (*Nederlandse Publieke Omroep*), a famous Dutch television channel, explains that every time that informal caregivers or financial administrators log in with the DigiD of the person they are helping, they are, in fact, committing identity fraud. All the interviewees successively describe how DigiD is inconvenient for them as much as for the persons they are helping, therefore adding more difficulties to already difficult lives and jobs.

As I mentioned in the introductory chapter, the invisibles of DigiD also partly remained invisible to me. Therefore, let's introduce Amir, the first to have opened the doors to this other side of the DigiD interface.

Amir is a social counselor working and living in a neighborhood of Amsterdam-North where almost everyone is struggling with debt. Amir is in his late twenties and helps people from lower classes with their administration, and therefore uses DigiD every day. The people he assists all have a DigiD, he says, but all "find it difficult". He further explains:

> And it is the reality that sometimes it costs two or three appointments to just get all the papers ready. Like for example if somebody comes at the first appointment, most of the time, the DigiD is not working, or the password is incorrect and the people just don't know what it is anymore. Second time, when you ask for the new DigiD, they will send an activation code and third time, the person comes with the activation code but not with the username. Or people don't realize that capitals, or small letters, or things like that are important. So it's just too much for the people to handle. And especially because of the transition… before everything was done with pen and pencils, and it was easier for the people to do it like that. And the transition to go immediately to the internet, it is going very fast and too fast for these people who are coming here, yes.

Although now, it is a truism to say that this statement radically contrasts with the experiences of my previous wealthy and/or educated users, this login moment is the perfect example of DigiD accentuating bureaucratic hurdles. First, DigiD still heavily depends on paper, or more precisely, on letters. Although the first step of the application process must be done online, the

[17] "DigiD is unsuitable for informal caregivers," Meldpunt, NPO Start, accessed July 31, 2021, https://www.npostart.nl/meldpunt/20-11-2020/POW_04626988.

second step consists of waiting for a letter containing the activation code. The letter is sent to the same address that the applicant gave to the Dutch Personal Records Database (BRP). If the address has changed and has not been previously communicated by the applicant, the latter has to first contact his/her municipality to modify the address before re-asking for a DigiD. The application code is valid twenty days, after which, the applicant will have to reapply for a DigiD. And if users decide to call the DigiD helpdesk to try to retrieve their lost or forgotten login credentials, they are simply told to apply for a new DigiD, as the helpdesk's agents are unauthorized to access this private information. Although all these steps are the same for all DigiD users, my wealthy and/or educated users did not mention any of this during our interviews. In fact, Amir points out something that wealthy and/or educated have, in contrast, easily assimilated: the precision that login credentials require from their users. Users have to be impeccably exact when they type their password and username. In this sense, DigiD is a "utopian" system – as Graeber (2015, 48) would say – because as any form of bureaucracy - "they propose an abstract ideal that real human beings can never live up to and refuse to deal with people as they really are".

Dirk – another social counselor helping the most vulnerable people of Amsterdam-East for more than thirty years – explains how this login process is debilitating as it creates superfluous problems not only for his clients but also for himself:

> For us it gives a lot of extra work in fact. It's not difficult work but it's too easy. Because I studied law but a big part of my time, I'm asking for DigiD and thinking of – oh this DigiD does not work, how should it be so then it works? All these things are extra, and not complicated, but extra work, and yes… it's not necessary.

Or, in Graeber's (2015, 48) words: "bureaucratic procedures have an uncanny ability to make even the smartest people act like idiots". Instead of solving real-life related issues, social counselors like Amir or Dirk spend most of their time dealing with technical problems. Let's recall that DigiD, as an authentication service, was precisely created to alleviate government organizations from these problems. Yet, what we can draw from these statements is that DigiD – as a digital form of bureaucracy – has, in turn, outsourced its inherent bureaucratic hurdles to social counselors. As I described in the opening vignette of this thesis, the invisibles still sit in the waiting rooms of the social centers where Amir and Dirk work. They might not wait in the lines of government buildings, but they do wait for a letter to arrive every time they forget or lose their login credentials. However, DigiD further reinforces bureaucracy as it transforms, for

the invisibles, the most basic action of showing someone their identity papers – since this is exactly what DigiD consists of – into something impossible, or at least, immensely complex and confusing.

Another quintessential example of the digitalization of bureaucracy as reinforcing bureaucracy is the proliferation of call centers.

Masiko is one of the invisibles of DigiD. In fact, one of the few I could gain access to, and we have Amir to thank for that. Amir has been Masiko's social counselor for two years. Masiko is a thirty-year-old single mother of six who emigrated from Uganda five years ago, and obtained asylum for her and her children. She remembers how, in Uganda, she would directly go to the concerned office and always leave with an answer. But in the Netherlands, Masiko has to deal with call centers, which truly annoys her. Masiko explains that, every time she tries to reach an organization, she has to speak to five different persons who keep sending her from one to another: "No you have to call my *collega* ["colleague", in Dutch], you have to ask this *collega*, I'm gonna ask my *collega*, *collega*, *collega*". Besides dereliction, Masiko therefore starts thinking that she cannot do it by herself, "forcing her to ask for help [...] which is not an easy thing to do", she adds. But what is particularly interesting in Masiko's story is that, compared to most of Amir's or Dirk's clients, she does have a smartphone and a computer, which she both knows how to use. Although Masiko seems to have passed the test of digital inclusion, she still has to ask for Amir's help when arranging things with her DigiD. Indeed, she is "afraid to miss something", which would jeopardize her and her family's entire nationality application process. Amir also helps Masiko decoding the many official letters she receives, even though she speaks five languages, including Dutch and English. No matter how brave, resilient, independent, and skillful she is in life, Masiko still have to face bureaucratic hurdles, which are exacerbated by her social vulnerability.

Finally, DigiD exemplifies what Graeber (2015, 53) calls the "absurdities of bureaucratic life".

First, it is quite common for Dirk to fill in paper forms because the digital forms are not adjusted to his clients' situations. Yet, Logius writes on its website:[18] "With DigiD, the customer [the organizations] can immediately check what information he already has about this

[18] "Functional Description of DigiD," Logius, accessed August 1, 2021, https://www.logius.nl/diensten/digid/documentatie/functionele-beschrijving-digid.

person and can offer his services tailor-made". However, DigiD does not offer tailor-made services for the invisibles. In fact, DigiD does not even offer anything to these invisibles who are forced to "fill in a form like thirty years ago, and then send the form to them", says Dirk.

Second, the fact that every time that Amir or Dirk are helping their clients they are committing identity fraud is, perhaps, the biggest absurdity of this digital form of bureaucracy. As we recall, DigiD provides organizations with the absolute guarantee about the user's identity, and must therefore remain strictly confidential. In the documentary by NPO, a woman explains that, although she has power of attorney over her seventy eight year old mother, Logius does not recognize this notarial document and qualifies this help as illegal. Although discussions with Logius on this issue are ongoing, this bureaucratic "stupidity" (Graeber 2015, 57) makes it harder for the invisibles to get help, rendering them, perhaps, even more vulnerable.

Therefore, DigiD – as a digital form of bureaucracy – is for and foremost another bureaucratic tool rather than a new digital technology for overcoming bureaucratic barriers. We have seen how DigiD generates sharply different outcomes, based on one's socio-economic position. Indeed, if DigiD can be experienced as liberating by wealthy and/or educated users, it is "alienating" (Gupta 2012, 14) for the invisibles as it creates even more disparities. However, what is slightly different – and perhaps even worrisome - in this new digital form of bureaucracy is that this disparity is imperceptible by the rest of the Dutch population.

From digital inclusion to digital exclusion

After two months of fieldwork, I initially thought that illiterate people and the elderly were the main people that were excluded from the digitalization of bureaucracy and that the work of libraries and foundations, such as Digisterker, would assist them in this process. Yet, as we now stand on the other side of the DigiD interface, can we be certain that the invisibles can access these helpful resources?

When Amir tells me that many of his clients "don't have a computer, don't know how to use it, and cannot learn how to use it", I ask him if these clients know about Digisterker, or participate in any other library courses for developing one's digital skills. He straightly answers: "that is a different kind of people who go to library courses". To be honest, it is only after this

statement that I have recalled something that Jacqueline, the librarian/teacher, told me during our interview:

> So at the moment, my participants are people who are over seventy. With Dutch background, sometimes very good in… of course they have money, they have a high level in education but not so high level in digital skills.

As we juxtapose Amir's and Jacqueline's statement, it becomes clear that Amir's clients will never attend Jacqueline's, or any other librarian's, course. But Amir goes further into his explanation:

> And a lot of organizations that are providing computer classes, for example, it's also in the policy that you can't go two or three times too late otherwise then it's over. For those people who are coming here, who are really suffering every day, who are really thinking about how can I survive today and how can I support food for my children the next day, they cannot think about everything. It is really short-term. And for those people there are some projects who are committed very better than the library courses

Amir shares how the invisibles have too many problems and not enough time to be able to commit to these courses. But more importantly, Amir brings our attention to the structure and the organization of these courses that do not seem to work for everyone, especially for his clients.

Although it is usually for free (or maximum €20 for the entire course), a Digisterker course consists of three to four lessons of two hours each. Lessons mainly take place on weekdays between 8 a.m. and 4 p.m. Some libraries do offer night classes, but for this group of people, this entails attending such sessions after their job and having to arrange care for their children, which would be quite a commitment.

Moreover, to enroll into a Digisterker course, students must have some prior digital knowledge. Most of the libraries write – on their website - in the course description "we assume that you already have some experience with computers and the Internet".[19] A library called

[19] "Digisterker," Gemeente Enschede, accessed August 1, 2021, https://www.enschede.nl/onderwijs-en-kinderopvang/digisterker.

"Bibliotheek Oost-Achterhoek" (*Achterhoek* being the name of a region in the eastern Netherlands) even created a digital test – Digistest – that potential students can take in order to determine whether they have "sufficient knowledge to participate in Digisterker".[20] If we look at the ten questions of this test (see appendices D), we realize that this course is quite selective. I passed this test with a score of 70 points out of 100, which is quite self-explanatory for our argument, namely – digital inclusion courses like Digisterker are not made for everyone, and certainly not for Amir's clients.

In an explicative brochure of the course,[21] it is stated that these lessons are taught in Dutch and require a B1 language level. Before 2018, Digisterker only offered course material that required C1 level in Dutch. However, when Amir does not help his clients with their DigiD, he spends the rest of his time decoding and explaining official letters, which gives us an idea about the literacy level of this group of people, who are maybe not able to follow these courses for the same reason. Also, is this group of people used to going to libraries, in their leisure time? And do they have any leisure time?

In addition, these courses seem quite scholarly. Students receive a booklet that they use during and after the course. Students have homework to do in order to earn the Digisterker certificate and must practice on their own computer at home (again – assuming they do have a computer, and the time to do that). Although all libraries write in their course description that they "do not need to take an exam",[22] sessions are punctuated with little quizzes. For the invisibles, it is a bit like going back to school after having been failed by a lack of resources in their first experience of school.

Finally, as I was looking at the different subjects approached by the Digisterker courses, one of them particularly caught my attention. Indeed, during these courses, students also learn how to use the DigiD app. However, when I asked Amir and Dirk about the DigiD app both made it very clear that none of their clients had it, or at least, that they never used it with them. The DigiD app seems to be exclusively reserved to the wealthy and/or educated users, whether they use it or not. This can be explained by the fact that the DigiD app requires its users to have a recent version of a smartphone. For example, the DigiD app cannot be downloaded on an

[20] "Digisterker," De Bibliotheek Oost-Achterhoek, accessed August 1, 2021, https://www.oostachterhoek.nl/digisterker.html.
[21] "Digisterker," Bibliotheek Netwerk, accessed August 1, 2021, https://www.bibliotheeknetwerk.nl/basisvaardigheden-volwassenen/digitaal/werken-met-de-e-overheid-digisterker.
[22] "Digisterker," Gemeente Enschede, accessed August 1, 2021, https://www.enschede.nl/onderwijs-en-kinderopvang/digisterker.

iPhone 7 (which was released on September 7, 2016) or older version. Let alone the whole two-factor authentication process divided into three steps: with the pairing code, the QR-code, and the PIN code.

Therefore, it seems that the Digisterker courses are very selective in the choice of their students, as if the pre-requirement for digital inclusion were social inclusion. As we stand against the proposition that technology has a linear impact on people and society (Rao 2013), we understand that digital exclusion is nothing but the replication of the same pre-existing inequalities inherent to the Dutch society. The invisibles of DigiD are thus locked into a vicious circle as their social exclusion generates their digital exclusion, which exacerbates their social exclusion, and so on.

Indeed, digital inclusion paradoxically creates more social exclusion by stigmatizing those who do not have the same resources as wealthy and/or educated users. Amir shares how his clients experience this digital exclusion:

> People who are not capable to do things themselves, they almost have an etiquette or a sticker which says – you don't want to do it. But there are so many reasons why somebody cannot do it, and it is only yes or no, but I think there are so many answers between the yes or no.

As we recall, DigiD – as a form of governmentality – values individualism and self-determination. Therefore, "failures to get what one wants suggest moral deficiency and demand self-justification" (Herzfeld 1992, 4) as if class distinctions did not cause any "prejudice" (Rao 2013, 75). So, If DigiD – as a class affair – continues to exclude the most vulnerable people of the Dutch society, it goes one step further into this exclusion as it renders this group of people invisible.

The promotion of digital inclusion has resulted in the invisibilization of the most vulnerable people of the Dutch society, who only appeared in the national discourse as stereotypes. In fact, these stereotypes are paradoxically vague. For instance, every brochure or article on digital inclusion always starts with a statement like this one "around 2,5 million Dutch

people find it difficult to use digital devices"[23] – taken from a brochure published in 2019 by the Digital Government, a website commissioned by the Ministry of the Interior and Kingdom Relations (BZK) and intended for professionals working on the digitalization of the government. This statement begs for a series of questions: who are these 2,5 million? What about foreigners living in the Netherlands who are not officially Dutch citizens? What do they mean by "difficult" and why do they find it difficult? Do they have any digital devices on which they can practice? Do they have people who can help them at home? If not, why? And why the approximate number? Is this estimation based on surveys with librarians like Han or with social counselors like Amir? Are the invisibles of DigiD included in this estimation? If we continue to read that brochure from the Digital Government, two words besides the vague descriptor of "people" are used: "illiterate people" and "disabled people", which do not match Amir's or Dirk's descriptions of their clients. In fact, as I said earlier, the invisibles of DigiD were invisible to me for the majority of my fieldwork because of these generalizations, and thus, invisibilization.

Finally, although librarians and foundations, such as Digisterker, aim to ensure everyone's participation in society, their digital inclusion strategies do not even reach the most vulnerable people of that society. Therefore, we can better understand why my librarians in the previous chapter said regretting "not having enough students". The problem is less that not enough people go to libraries, but more that library courses are only structured and organized in a way that only attracts and accepts the same wealthy and/or educated people while rejecting people from a lower socio-economic position. And because, in this governmentality network, libraries serve as local branches supposed to identify possible dysfunctions and relay these to the Dutch government, the most vulnerable people of the Dutch society become and remain – *invisible* – more than excluded – as they never get through the door of these digital inclusion courses.

[23] "Digital inclusion: Everyone must be able to participate," Digital Government, accessed August 1, 2021, https://www.nldigitalgovernment.nl/wp-content/uploads/sites/11/2019/02/digital-inclusion-everyone-must-be-able-to-participate.pdf.

DigiD or DYE: from self-reliance to dependence

> So a couple years ago, I was at some gathering for older people, and they were very angry! They said – we cannot use it! We don't know how to use this! We cannot learn it! and nobody wants to help us! And they were angry about it! And they said – now in fact we, in the past, we could manage things on our own but now we are dependent on others who can help us with this. So in fact, for these groups, it does not make it easier, but it makes it harder and more dependent in fact that they were before.

Although Dirk relates a discussion he had with a group of older people, his statement sheds light on this other side of the DigiD interface – one that radically contrasts with the governmentality ideals of independence. Let's recall that DigiD – as a form of governmentality – rests on and thrives into self-reliance, that is, one's individual capacity to govern oneself. So if this new technology is supposed to have transformed Dutch residents into fully self-governing individuals, how does it impact those who do not – because they cannot – comply with it?

Dirk first points out that the invisibles, and especially older people from that group, simply "don't know how to use" DigiD and "cannot learn it". Indeed, Nadine's experience echoes what Dirk says.

Nadine is an informal caregiver for her eighty-five years old mother. Her mother used to have several jobs. Although she trained as a dressmaker, she ended up working in grocery stores, camp sites and as a housekeeper in guest houses. Due to the nature of her jobs and to the fact that her deceased husband was more interested in learning digital skills than her, Nadine's mother never learned how to use a computer nor a mobile phone, let alone a smartphone. Today, Nadine's mother cannot walk nor drive anymore which makes it difficult for her to attend one of the Digisterker's courses. Nadine's mother "hardly knows what DigiD is". Nadine then adds:

> If everything was still on paper, my mom could do more herself, as far as the administration is concerned, because she simply cannot use the computer.

Nadine's mother's experience resonates with Sora Park's (2017, 27) idea of "digital capital", which refers to "a predetermined set of dispositions that influences how people engage with digital technology". Indeed, if Nadine's mother does not engage with DigiD, it is because she never had to engage with any other digital technologies before. Yet, as the word "capital"

implies, one's experience of digital technologies is accumulated over time. For Nadine's mother, to start using DigiD would mean to learn a new form of knowledge. She would have to engage into a learning process that, perhaps, would require more time and energy than she really has. Moreover, because of Nadine's mother's lack *of* digital skills, she becomes dependent on her daughter. Inversely, one's digital knowledge is "capital" because it adds value to the individual. Park's (2017) concept therefore accounts for the experiences of the wealthy and/or educated DigiD users showing that, once again, one's social and economic status shapes one's experience of digital technology, and thereby one's perceptions and experiences of DigiD.

If we go back to Dirk's statement, we understand that people who lack resources to engage with DigiD also end up feeling "powerless" as "nobody wants to help" them. Both social counselors identify "powerlessness" or "abandonment" as the most characteristic feelings of the invisibles' experiences. Dirk goes further into his explanation:

> In the past, you could go and meet with somebody and they could help you, but now, no. They will not help you anymore. They say – do it by DigiD, and if you cannot do it yourself, you find someone to help you. So they all say … you can get lost. We don't help you anymore. That's the message that all institutions give these days! And in the past it was different, you could have contact with people.

Dirk explains that, today, if Dutch residents want to communicate with the government, it can only be done digitally. So when vulnerable users cannot use their DigiD and thus cannot communicate digitally with the government, they feel as if they were deserted and thereby feel powerless. DigiD – or Do It Yourself – finds resonance again in Herzfeld's (1992) concept of "social production of indifference". As interactions between bureaucrats and vulnerable users are quasi - if not totally – inexistent, the state can "insulate itself from social suffering" (Herzfeld 1992, 5), more than ever. On the same subject, Amir adds:

> What we see are people who cannot sleep because of this. Because we are seeing the reality here, if somebody comes in, it's really stressful and it's a bad thing because stress also gives mental and physical problems.

Indeed, Amir and Dirk are both on the front line of this abrupt digital transition that causes immense anxiety for already vulnerable people. But what Amir implicitly says is that the state

does not see those who suffer from DigiD. The digitalization of bureaucracy does not only reproduce the same mechanisms of indifference that shield the state from social suffering but further generates the *digital production of invisibility*. Simultaneously, the most vulnerable users are rendered invisible by DigiD as they are unable to connect or to reach out to organizations; and the state does not see these most vulnerable users, making them, perhaps, even more invisible and vulnerable.

However, we remember that my wealthy and/or educated users also mentioned this lack of human contact during our interviews. Yet, it does not provoke for them the same disturbing outcomes. In fact, even with the invisibilization of the state (and maybe especially because of it), wealthy and/or educated users are still able to find empowerment, freedom, happiness, agency, advancement, and well-being in this form of governmentality. In fact, now that we stand on this other side of the DigiD interface, now that we have lifted the cloak of invisibility, we can see that the state is not a "coherent nor unified entity" (Rao and Greenleaf 2013, 286). The experiences of the invisibles come to dismantle the governmentality machinery of DigiD as they shatter any illusion of cohesion and unity on which the state rests. With Gupta and Sharma (2006, 11), we think that "what the state means to people is profoundly shaped through the routine and repetitive procedures of bureaucracies". Through this lens, we can see that, for instance, every time that the invisibles fail to log in with their DigiD because their credentials are incorrect, it shapes their perception of the state – which is a state that does not grant them access. Every time that Amir's clients ask him to help them arrange things with their DigiD, it shapes their understanding of the state – which is a state that does not assist them. The more DigiD distances our invisible users from the state, the more our invisible users have a distorted perception of the state. And the less they can rely on the state, the less they trust it. In other words, DigiD erodes the trust of vulnerable people in the state, thereby making them, perhaps, even more invisible. But Dirk concludes our interview with an alternative and hopeful view as he says:

> But yes… there is no trust. And it's also part of my job to show the citizens that it's still possible to be in contact or whatever, even if it's digitalized, with government and institutions. And that it is possible to get what you want, or what you are entitled to, in fact. So part of my job, as I see it, is also to restore the trust of the people in institutions in fact. But it should not be that way. It should not be necessary that I would do that. But that's I think part of my job…

Amir and Dirk both reassemble the pieces of a fragmented state. Wouldn't that be what "governmentality" (Foucault 1991) ultimately is? Yet, we have seen that the governmentality machine tends to reproduce the same pre-existing inequalities, so can we even dare to hope that these same Foucauldian mechanisms would restore what they have already shattered?

Conclusion

To sum up, the multiple experiences of the invisibles unveil what is, maybe, the most paradoxical effect of DigiD. Rather than connecting Dutch residents to the state, DigiD disconnects those who cannot comply. Rather than being an interface, DigiD builds a border between vulnerable users and the state, whereas it is a point of communication for wealthy and/or educated users. Besides creating invisibility, and even more vulnerability, DigiD is just a new technology that serves as another bureaucratic tool having the same old utility: protecting bureaucratic structures and class privileges.

Yet, as a new technology, we should guess now that it also comes with its set of effects, ones that remain partly invisible to the Dutch society, and maybe, or to any society adopting a digital bureaucracy.

Chapter 3: The Invisibility of DigiD

Two weeks before the beginning of my fieldwork, RTL Nieuws – a famous Dutch television news service – reported a data leak from the Public Health Service (GGD) of Amsterdam. This leak came as a bombshell and took center stage in the Dutch News. The GGD suddenly received thousands of calls from concerned Dutch residents asking how their own data could be used against them.

Indeed, RTL Nieuws discovered that the personal information of thousands of Dutch residents (such as address details, e-mail address, telephone number, and citizen service number) were illegally traded via Telegram, Snapchat, and Wickr. The GGD is the organization where, among other things, Dutch residents can get tested for corona. Although it is possible to arrange a corona test by telephone, most Dutch residents usually book their corona test online, which can only be done via DigiD. As discussed in the first chapter, one's DigiD is linked to one's personal information. Therefore, when Dutch residents book a corona test online, they automatically transfer their personal information to the GGD, which stores them in two corona systems called CoronIT and HPZone Lite. But how could the private information of thousands Dutch residents be leaked? In one click - literally. Indeed, before the discovery of this leak, the two corona systems used to have an "export" button, which any of the thirty thousand GGD's employees could arbitrarily decide to press. So, when two young men working at the GGD decided to steal the private information of thousands Dutch residents, they did not have to drag thousands of boxes of files from the back door of the building, in the middle of the night. Instead, they just walked out at the end of their day with an USB key in their pocket.

Introduction

In this last chapter, we will endeavor to perceive the intrinsic invisibility of DigiD and understand the effects that this invisibility can generate on DigiD users' perceptions of online security and data privacy. First, we will see how the state aims to responsibilize DigiD users also in their online security practices. Yet, we will notice that there is a discrepancy between security imperatives and the users' perceptions and practices of online security. We will then dive into the largely unknown and hidden DigiD security infrastructures, from Logius' point of view, to discover the potential insecurity that DigiD can create. I will then introduce my last

group of informants – the experts – to show that the governing and understanding of this digital form of bureaucracy requires a certain IT know-how that the majority of the Dutch population simply do not have. Lastly, we will unfold the indifference that most of my participants show towards data privacy questions and recognize the invisibility that DigiD creates as the root of this indifference.

"Keep your DigiD safe"

In the first chapter, I portrayed how Dutch residents are urged to become more autonomous and self-reliant as they arrange administrative matters online with their DigiD. However, this individualization process does not stop at bureaucratic affairs. In fact, Rose and Lentzos (2009, 234) argue that this "autonomization and responsibilization of actors" also intervenes in the governing of security. Therefore, DigiD – as a form of governmentality, or "advanced liberalism", as Rose (1999) prefers to call it – also involves for its users a novel way of framing security as they start using this new digital technology. For instance, on the DigiD's website,[24] users are given some "security tips to use DigiD securely". Users are asked, for example, to choose a "complex and hard-to-guess" password, never share their login credentials with others, or to install an "effective security" on their PC and to always use a "secure connection when using DigiD".

Librarians who teach Digisterker courses also have a role in this responsibilization process. Let's recall Jacqueline, the librarian and Digisterker teacher from the first chapter. She says that "safety is not a fun part of the course, but it's a very important topic". She adds, "I will show you that it's safe, and I will show you how you should do to keep your DigiD safe". As her students starts to feel digitally self-confident, they can therefore start governing their own security for their own well-being (Rose 1999).

But users are also encouraged to police "any suspicious online activities" related to DigiD, and therefore protect the entire DigiD infrastructure. Via the DigiD website, users can report vulnerabilities of the DigiD IT systems and phishing attacks. Phishing is a technique used by hackers designed to trick victims into revealing sensitive information to the attacker. It often takes the form of an official email or SMS. Victims are asked to click on a link and/or provide personal data. These messages usually play on people's fears and weaknesses. For instance, victims are told to respond immediately if they do not want their DigiD account to be

[24] "Security tips," DigiD, accessed August 1, 2021, https://www.digid.nl/en/prevent-abuse/security-tips.

terminated, or to click on the link contained in the message to receive, what usually is, a fair amount of money. If victims do click on the link, they are redirected to a fake DigiD website that looks like the official one. The main victims of these hackers are, perhaps, the invisibles of DigiD, since most of them struggle with debt and none of them are digitally experienced enough to recognize a fake from an original website. But digitally literate users can report these vulnerabilities via digital forms on the DigiD's website, e-mail, or most commonly via Twitter. DigiD's Twitter account, @DigiDwebcare, receives hundreds of tweets every month that notify phishing attacks. The number of cyber-attacks has exploded during the corona pandemic. Logius has taken more than 2500 DigiD phishing sites offline since the start of the corona pandemic.[25] Twitter-users publish screenshots of these phishing attacks and tag the @DigiDwebcare. Other members of the community then retweet these tweets, which generates for users a "perpetual alertness and individual preparedness" as they become DigiD's "guard against the emergence of any and all possible threats" (Goldstein 2010, 492).

Yet, although Goldstein (2010, 492) identifies "suspicion" as the new "disposition of the neoliberal subject in this security society", I honestly cannot say the same for my informants. Rather than being "prudent citizens" (Rose 1999, 166), my informants tend to be more credulous, and even lazy, when regarding the security of their DigiD.

Convenience rather than security

Sasha – one of my wealthy and/or educated informants – speaks for all my participants when she says, "I use the same password for everything". And half-smiling, she continues, "that's like, not recommended, but then I don't want to forget it because it's too many. You can't make one every time." Most of my wealthy and/or educated informants have for all their online activities one or two passwords, which are automatically saved on their computer or smartphone, for practical reasons. In fact, when the invisibles write their login credentials on a piece of paper, as Amir or Dirk told me, they are perhaps less vulnerable than my digitally literate informants concerning their online security, even though they do not realize it. My wealthy and/or educated informants all know that they should be more careful with their DigiD and admit to it as if I caught them red-handed. During my interviews, we usually have this

[25] "DigiD and mijn Overheid are more often targeted by cyber criminals," Data & Privacy Web, accessed August 1, 2021, https://privacy-web.nl/nieuws/digid-en-mijnoverheid-vaker-doelwit-cybercriminelen/.

moment of complicity where I also admit to it, sharing the same clement/slight embarrassment that vanishes in a laugh as we jump to the next question.

In a report published by Rijksoverheid.nl in 2019,[26] we read that 84 percent of all logins on DigiD occur without using the second factor (2FA). As explained in the first chapter, the 2FA is more secure than the first login method, which is a username and password. Yet, the 2FA is not perceived as user-friendly by my research participants, especially Mariska – the Dutch Fashion Design student whom I introduced in the first chapter - who wanted to try the DigiD app before suppressing it from her iPhone. She says, "I was kind of disappointed because I saw that the app was just some extra security to log in on your computer, not more than that". For Mariska, security vis-à-vis DigiD even seems annoying and superfluous. But that is because, if we remember what Mariska said earlier, "on the computer with DigiD, everything is so clear that nothing can go wrong, actually". So is Mariska completely certain of the security of DigiD or does she just assume it?

In fact, it seems like my informants do not even think of security when using their DigiD. Toward the end of my fieldwork, as I was still trying to understand the DigiD's users perceptions of security, I began to get impatient and asked one of my informants:

> - Do you think DigiD is safe?
> - Yeah! I think it's really secure, I don't know if it's not but I think that it's good.
> - Ok, did you already tell yourself once like – oh! It's safer than in England? Do you make comparisons sometimes with England?
> - To be honest, not much. I have never thought that way, in terms of security and everything. So yes… I don't know how to … (laughs)

From this quote and based on my other interviews, it becomes clear that DigiD users do not think of DigiD in "terms of security", or at least, in terms of insecurity. Or perhaps they do think of DigiD in terms of security – namely, " the freedom from danger, fear and anxiety".[27] In fact, Amir was the only one to address the theme of security, although he did it through the insecurity that DigiD can create:

---

[26] "Report Monitor Digital Government 2019," Rijksoverheid, accessed August 4, 2021, https://www.rijksoverheid.nl/documenten/rapporten/2019/06/30/rapport-monitor-digitale-overheid-2019.

[27] Dictionary Merriam-Webster, s.v. "Security," accessed August 4, 2021, https://www.merriam-webster.com/dictionary/security.

> We have also one case of a woman who trusted her pastor, priest with everything. He was a father with whom she'd go every Sunday and the pastor told – give me your DigiD because you have a lot of problems with debts. So the pastor told – you know give me your DigiD and I will sort it out. And what he did, he asked for PGB [*persoonsgebonden budget*], it's some kind of money you can ask if you help people for illnesses, and he used everything in her bank account. He took somewhere around 100.000-200,000 euros. He left and the woman is alone and the woman cannot do anything because it is her DigiD that he used. So she gave her DigiD to somebody and that is… then you can see that the movement is way too far.

Amir calls our attention to the fact that the invisibles – and this applies to all my participants – do not consider DigiD as their "digital identity". So, when this pastor asked this woman to give him her login credentials, she did not realize that, in fact, she was giving him her digital passport or ID card. And because DigiD aims to provide organizations with a certain degree of certainty of the identity of the person who is logging in, there is, unfortunately, no solution for this woman. She gave someone else access to her DigiD although she was never supposed to. She thought she was safe because she *trusted* that pastor.

So, rather than looking at the insecurity of DigiD, we should try to understand what makes my informants think it is secure, or unknowingly assume that it is. The feeling of trust appeared in many of my interviews. For instance, Masiko – my invisible user whom I introduced in the second chapter – does not feel unsafe as soon as she gives Amir her login credentials. In fact, she says that Amir is the "only one [she] trust[s]" for handling her administrative life. She feels unsafe when she cannot contact government organizations or receives a letter that she does not understand. But when she visits Amir, she feels safer than before because she is finally cared for.

Or let's take our librarian Han from the first chapter. During his Digisterker classes, he describes teaching his students "how to keep their DigiD safe". Yet, he adds that he tries "not to overstress this security during courses because then they [the students] become afraid to use the computer". Therefore, DigiD seems to rest on a fragile equilibrium between trust and security. If users would start fearing for their safety, the whole delivery system of the state would stop working as Dutch residents would stop trusting it. Every time that Logius adds a new login method to DigiD, they subtly stress that it is the "safest" instead of "safer".[28] When

[28] "Login methods," DigiD, accessed July 29, 2021, https://www.digid.nl/en/login-methods.

users are nudged into taking their security "into their own hands" (Goldstein 2010, 498), the state thereby ensures the sustainability of DigiD itself. In short, trust and security are inextricable.

Invisible (in)security

At this point, we might think that the entire security system of DigiD comes down to the users themselves. In fact, the responsibilization process of DigiD users aims to safeguard their trust, rather than the DigiD's internal IT system that consists of, in fact, an immense web of public – but mainly private – institutions. Users do not see behind the DigiD's logo and login page, and there is nothing they could have done to prevent the leak of their data at the GGD, for example. The digitalization of bureaucracy and its sustainability rests on an entire international infrastructure that remains invisible but also almost impossible to understand for anyone who is not an IT expert.

Let's start by stating that in cybersecurity, total security is an illusion: security is about evaluating and mitigating risks (Woolward 2017). Indeed, Logius requests every year from their clients a risk assessment evaluation of their IT system. Organizations must themselves pay for the cost of this annual audit, which is done by third private parties. Yet, if the GGD leak that I described in the opening vignette of this vignette happened it is also due to the fact that the GGD's website failed to meet on three occasions Logius' security requirements. But, in these pandemic times, no one could afford to lose access to the GGD website.

Logius itself outsources the management and organization of its IT infrastructure and security to private IT suppliers (for the list of suppliers, see appendices E). These suppliers must also respect a certain number of privacy rules to be able to access the DigiD's IT system, which certainly generates more contracts, more employees and thereby more bureaucracy. Although this list of suppliers is public, I could not really understand what role each of them exactly plays in the maintenance of DigiD.

DigiD also rests on database centers, also called "hosting companies". The Netherlands is one of the biggest hubs of data centers in Europe.[29] Yet, less than a third of these data centers

[29] Diederik Toet, "Restriction of data center not disadvantageous for the Netherlands," Computable, accessed August 4, 2021, https://www.computable.nl/artikel/nieuws/datacenters/7207354/250449/beperking-datacenters-niet-nadelig-voor-nederland.html.

are used for organizations based in the Netherlands.[30] Government organizations store their data in these hosting companies, as if they were renting a storage unit. These hosting companies are scattered throughout the world, which means that a Dutch municipality can rent some data storage to the US, for example. Although some hosting companies can get access to the data they store, it does not seem to apply to the data of Dutch organizations. [31] However, if we look at the IP address of DigiD (144.43.243.208),[32] we see that it is based in the Netherlands. DigiD runs on servers owned and managed by Logius. However, Logius rents its network connectivity, which is basically like renting an internet connection – like we do at home – from various big data centers throughout the world.

But the most quintessential example of the invisible (in)security of DigiD is, perhaps, the case of PKI (Public Key Infrastructure), also called "trust certificates". Trust certificates are used not only for DigiD, but for any webpage. In very simple terms, every time we visit a webpage, our browser checks whether the page being loaded is really the page we wanted to access, and not a fake copy of that webpage. In case you ever wondered, this is what the little lock on the left side of the URL in our browser means. We usually notice it when it becomes red as it warns us not to trust a site, although most of us have probably clicked through such warnings. So, because every website does not want to be responsible for this trust screening process, they rely on third parties that vouch for the authenticity of each website by issuing these trust certificates. More specifically, when an organization wants to use DigiD, they have to buy trust certificates from Logius, which Logius buys from Getronics (see appendices A.3). However, in 2011, one of the biggest hacks happened in the digital world. Before Getronics, Logius used to buy all its trust certificates from DigiNotar, a well-trusted and reputable certificate authority. DigiNotar was extremely protected from hackers virtually, but also physically. Each new certificate had to be vetted by two DigiNotar employees. Then, to issue the new certificate, one employee had to go insert a physical key card in a computer located in

[30] "Exploration of relationship to accommodate data center demand and digitization opportunities," Rijksoverheid, accessed August 4, 2021, https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2021/06/14/verkenning-relatie-accommoderen-datacentervraag-en-digitaliseringskansen/Verkenning+relatie+accommoderen+datacentervraag+en+digitaliseringskansen+-+eindrapport.pdf.

[31] Arnout Veenman, "Hosting DigiD in foreign hands? No of course not," Ispam, accessed August 5, 2021, https://www.ispam.nl/archives/52723/hosting-van-digid-in-buitenlandse-handen-nee-natuurlijk-niet/.

[32] IP Info, s.v "DigiD", accessed August 5, 2021, https://ipinfo.info/html/ip_checker.php.

a heavily-guarded room, as described in a report commissioned by the Dutch government to investigate the cause of the hack:[33]

> This room could be entered only if authorized personnel used a biometric hand recognition device and entered the correct PIN code. This inner room was protected by an outer room connected by a set of doors that opened dependent on each other, creating a sluice. These sluice doors had to be separately opened with an electronic door card that was operated using a separate system than for any other door. To gain access to the outer room from a publicly accessible zone, another electronic door had to be opened with an electronic card.

As of today, it has not yet been ascertained how the intruders could have bypassed all the physical security put in place. But what we know for certain is that this or these hacker(s) forged 531 trust certificates, mainly used to create fake Google webpages. This hack affected 300,000 users, of which 95 percent were Iranians. But what concrete impact did this hack have exactly? Hans Hoogstraasten, the team leader of the same previous Dutch investigation, gives us an idea of the consequences that these forged certificates might have had. He writes in an email:[34]

> What really shocked me was when I realized the impact it had for the people of Iran. In those days … people got killed for having a different opinion. The hackers (presumably the state) had access to over 300,000 Gmail accounts. The realization that the … security of a small company in Holland [may have] played a part in the killing or torture of people really shocked me.

Although I could not find any circumstantial evidence that verifies his claim, this hack shows how largely hidden infrastructures that tell our computers – and by extension us, blind users – who to trust, can make decisions that affect the entire security and safety of the Internet. After the leak was discovered, Logius immediately revoked its trust in DigiNotar, which was declared bankrupt, then dissolved six months later. And that is why, ever since, Logius buys its certificate from Getronics.

---

[33] "Black Tulip," Radboud University, accessed August 5, 2021, https://www.cs.ru.nl/E.Verheul/SIO2019/black-tulip-update.pdf.

[34] Josephine Wolff, "How the 2011 hack of DigiNotar changed the Internet's infrastructure," Slate, accessed August 6, 2021, https://slate.com/technology/2016/12/how-the-2011-hack-of-diginotar-changed-the-internets-infrastructure.html.

This hack illustrates how the potential insecurity of the digitalization of bureaucracy remains invisible for the quasi-totality of the population, which is certainly worrisome in cases like DigiNotar. But what this example of trust certificates also shows is that the governing, or even the understanding, of digital bureaucracies requires a real IT expertise.

"You don't understand what DigiD is"

During my fieldwork, I created a topic on a forum called security.nl to discuss in detail the (in)security of DigiD. Some users of that community came together and posted anonymously to enlighten me on these questions of (in)securities. I call them "the experts". As I said in the introductory chapter, the experts are who some might call "geeks". It was very challenging to discuss certain issues with them as they use a very specific technological jargon. For instance, as I refer to the four different login methods of DigiD and ask "why does not Logius provide the only safe way to log in?", one of the experts bluntly answers, "because there is no such thing". Another expert joins the conversation and asks: "why doesn't DigiD support a generic OTP [one-time password] generator/authenticator like many other websites/services do?". If we could all try to understand the question, I am not sure I could say the same concerning the answer:

> A generic OTP generator adds a second factor. DigiD currently uses SMS control and the DigiD app for this. Some OTP solutions use a special app. In the coming years, Logius will increasingly move towards the eIDAS reliability level in the Netherlands when logging in. TOTP cannot provide this level. If Logius were to use TOTP, this would mean that people would need both an OTP app and the DigiD app to log in at multiple reliability levels.

From this quote, the only thing that is clear is that the understanding of DigiD's IT systems requires a certain IT know-how that the majority of Dutch residents do not, and will never have. In fact, one of the experts even told me, "you don't understand what DigiD is". Although back then I panicked, today, my ignorance and his crudeness both make my point: understanding DigiD and using it securely simply seem impossible for us, mundane users. No matter how many hours we spend on our computers and smartphones, or if we are writing a master's thesis on DigiD, it appears that the core of that digital bureaucracy is not only imperceptible but also

unknowable. Perhaps, this is what Park (2007) ultimately means by "digital capital". In this case, those who have the most "digital capital" are the only ones who can understand "the impact and consequences of digital technologies in our lives" (Park 2007, 6). But this required expertise is even more worrisome when it is detained by a handful of citizens like my experts, who decided to remain anonymous and somehow invisible.

If digital bureaucracies are promoted as being more transparent (Alshehri and Drew 2010, Dandurand 2019), the question is to whom? Instead, digitalization makes bureaucracies more opaque. Already a century ago, Weber (2019 [1922]) identified "secrecy" as an inherent characteristic of administrative institutions. For Weber (2019 [1992]), secrecy is a functional necessity. He argues that "every bureaucracy seeks to increase the superiority of the professionally informed by keeping their knowledge and intentions secret" (Weber 2019 [1922]), 225). So, when the experts decide to remain anonymous, or when we learn about trust certificates being kept in a mysterious room that seems to come straight out of a science fiction movie, we start realizing that digital bureaucracies are just more sophisticated versions of "traditional" bureaucracies.

Perhaps, if my informants could see and understand the potential (in)securities of DigiD, maybe they would start being more alert, more prepared, and less indifferent to the safety of their new digital identity, like the public opinion's reaction to the GGD leak shows. Suddenly, Dutch residents became worried as they realized that, sometimes with DigiD, some things can go wrong.

I have nothing to see, so I have nothing to fear

During interviews, I often referred to the GGD incident that I described in the opening vignette of this chapter. I was hoping it would trigger for my informants a debate over issues of data privacy, as it did for me when I first heard about this leak. Yet, for my informants, the GGD incident was just another privacy scandal. In fact, one among the twenty-one thousand data leaks that were reported to the Dutch Protection Authority in 2020.[35] Although the GGD leak was a key event that received widespread media attention – perhaps because it was shocking

[35] "Reported data leaks doubled in the Netherlands last year," NL Times, accessed August 6, 2021,https://nltimes.nl/2019/01/29/reported-data-leaks-doubled-netherlands-last-year.

that the sensitive medical data of Dutch residents was leaked during these exceptional times of pandemic – it was by no means an exceptional case for the digital world nor my informants.

Not only did my informants not find this leak sensational, but they hardly felt concerned, even though I often tried. For instance, I could feel my participants faking interest as I was pressuring them for it: "how would you feel if the GGD was calling you to say that your information has been leaked and is now being sold on the darknet?", I would ask – dramatically. And half-smiling, they would answer, "well… I guess I would feel bad".

It is only toward the end of my fieldwork that I realized that the disregard of my informants toward privacy issues, and thereby towards my own interview questions on that subject, had been well-documented by sociology and law studies researchers and framed as the "I have nothing to hide, so I have nothing to see" argument (Lyon 2001, Marx 2003, Viseu et al. 2004). After I discovered the existence of this argument, I decided to create a focus group discussion. I wanted to see for myself if my informants' dismissal toward privacy issues could only be explained by the simple fact that they had "nothing to hide". So one night, with my boyfriend and eight of my friends, we all met at one of my friends' houses because she had a large dinner table that could fit all of us. This focus group discussion was composed of people of different ages – between 23 and 32 years old – and of various nationalities – Dutch, French, Mexican, and American. The following segments are from my field notes and the recording of the discussion I led that night while we were all eating freshly-made lasagnas:

> I put my phone at the center of the table, and I start with a simple question, or at least I thought it was - what is privacy for you? - One after another, my informants refer to things like "having my own free will", "something personal", "something secret", "something like a bubble", or "something that you wanna keep for yourself, but I think it's a choice". I realize that I should not have started with such an existential question. As a future anthropologist, I should have known, better than anyone else, that there is no such thing as a definition. Some of my informants even feel shy and start stuttering, "I dunno what else to say….". I see that some of my participants already start feeling less concerned about this, especially when Edouard says, "Privacy? Does it still exist? I don't think so".
>
> Before most of my participants give up on me, I decide to jump right in and say, "If you recognize yourself in the following statement, please raise your hand: I have nothing to hide, so I have nothing to fear". Five out of nine raise their hand. I then ask one of the participants with the hand raised: "why you don't care that the

> government, everybody can see everything?". Wrong question. But it's too late, I said it. So one of my friends immediately screams, "what? What are you asking? Are you referring to the government or to everybody? I don't want my mom to know that I'm watching porn!". Everybody laughs, and I feel stupid. I'm trying to rephrase when I decide to use that comment: "Okay, so who uses the incognito mode here and for what?". Everybody laughs again. We easily guess that everybody uses it for the same thing, "and for when I'm looking at flights! Otherwise, they raise their prices!", someone adds.
>
> Like always, Ximena and my boyfriend ended up arguing and monopolizing the discussion, which certainly was convenient for the rest of my informants who successively slipped from the dinner table to the living room, drinking wine and talking light.

At first, I was not sure about the outcomes of this focus group discussion. I resented myself for asking the wrong questions and for not having been able to retain the attention of all my participants. I could feel a general feeling of dismissal, resignation, and even annoyance emerging from my participants, like scholars had predicted. Also, it seems that the incessant apparition of privacy scandals, like the GGD one, only participates in trivializing these issues of data privacy. Indeed, Edouard is not only pessimistic: he is resigned. Therefore, it appears that DigiD – as a new digital technology bringing its own share of privacy scandals into the Dutch society – participates in creating more "social production of indifference" (Herzfeld 1992) vis-à-vis data privacy questions.

Even though that night of fieldwork confirmed that the Dutch residents' perceptions of privacy were pre-conditioned by the "I have nothing to hide, so I have nothing to fear" argument, I still was not completely convinced. Indeed, if my informants really did not care about their privacy, why would they suddenly be worried about their mothers' potential discovery? When the word "mom" came to substitute the word "government", I suddenly could feel the attention of all my participants, as if they could finally *relate* to something.

As I was going through my data, I realized that none of my participants knew what information their DigiD contained – except the DigiD makers (librarians/teachers or the representative from Logius) and social counselors. For instance, when I asked Mariska, she answered: "I've never really wondered what kind of information is on there… yeah… I think my… I don't even know". Or when I asked Pietro – another wealthy and/or educated DigiD user – he told me, "I guess a lot. All the personal information, who I am as a person, my… I

don't know. I think it's pretty bad, right?". Most of the time, my informants did not even bother to try and just admitted not knowing. For the majority, it was probably the first time they had to think about it, which temporarily generated for them an ambiguous feeling of embarrassment and apprehension.

Indeed, my informants had no idea that they could log in to mijn.overheid.nl[36] with their DigiD to view their personal data, under the rubric "identity". On that website, DigiD users can then see that their DigiD contains the following information: name, sex, BSN, date and place of birth, nationality, address, e-mail address, municipality of registration, names, data and place of birth of their parents, details of their children (if they have any), and if they ever connected to DigiD with their ID or passport, those will also be linked to their DigiD. In short, one's DigiD contains one's most basic and official identity information. After enumerating these information to my informants, they still could not *see* how a leak of this data could negatively impact them – or as one of my informants put it: "what the fuck are they [hackers] gonna do with it!".

Therefore, I argue that DigiD – as the digital production of invisibility – generates the "social production of indifference" (Herzfeld 1992) vis-à-vis data privacy questions. My informants do not fear anything because they cannot see anything. Therefore, the "I have nothing to hide, so I have nothing to fear" appears to be as dismissive as people's own perceptions of privacy. This difference stops to indifference without focusing on the reasons and the context of this indifference. Indeed, this argument is mainly used by researchers through the theme of surveillance. (Lyon 2001, Marx 2003). In situations of surveillance, the observed does not see – and sometimes does not even know about - the observer. And this argument does not take into account the invisibility, or at least the murkiness, of these surveillance situations. People might really be and say that they are indifferent, but that is because they do not feel threatened by something they do not know about. Indifference is what invisibility automatically produces. If Dutch residents were to see the direct consequences of a privacy threat, they would suddenly become more concerned. Although like for security, privacy only appears when it is - not threatened - but already attacked and thus, already too late. Let's conclude by imagining a different scenario of the GGD leak. What if, instead of being sold on the darknet, the data of thousands Dutch residents were to pave all the streets of the Netherlands with copies of their own passport, ID card, and the name of their parents and their children? Could not we suppose that my informants' reaction to this leak would be quite different as they would be able to *see*

[36] "Log in to Mijn Overheid," Mijn Overheid, accessed August 6, 2021, https://mijn.overheid.nl/welkom/.

the direct consequences of this leak - or as if they could finally recognize themselves in all of these bits of data?

Conclusion

Although we only remained at the surface of the DigiD's security infrastructures, we were finally able to perceive the potential insecurity of DigiD. Although DigiD users are firmly encouraged to secure their own online security, we have come to realize that the users' security is predicated upon largely hidden infrastructures that are barely understandable, thereby obscuring the Dutch residents' perceptions and understandings of online security. At the same time, digital bureaucracies further insulate themselves from citizens and outside control, as they require an almost secret knowledge that only IT experts possess. Lastly, we have seen that the digitalization – or invisibilization – of documents obscures the Dutch residents' perceptions of data privacy and, consequently, renders them indifferent to privacy concerns.

Conclusion

The aim of this research was to determine whether DigiD, as a digital form of bureaucracy, faces the same issues as non-digital forms of bureaucracies do. By focusing on the multiple experiences of DigiD users, this study has shown that DigiD does face the same issues as non-digital forms of bureaucracies, although some are exacerbated, and some are new. In order to illustrate this shift from non-digital to digital form of bureaucracies with their continuities, but also their novel effects, I primarily argued that digital bureaucracies, and more particularly DigiD – have gone from "the social production of indifference" (Herzfeld 1992) to the *digital production of invisibility*.

This study has shown that DigiD primarily constitutes an interface. On the one side, the digitalization of bureaucracy enables wealthy and/or educated Dutch residents with prior digital inclination to communicate more easily and autonomously with the Dutch government. Less digitally literate wealthy and/or educated Dutch residents are also easily absorbed into this new digital technology as they follow digital inclusion programs that are felt as empowering. DigiD is therefore primarily experienced as convenient due to one's socio-economic position and digital competencies, but also as enabling. DigiD, as a neoliberal form of governmentality, DigiD secures the ends of the Dutch government that aim to de-governmentalize its delivery of public service and the implementation in the society of DigiD. Indeed, we have seen how a multiplicity of non-state actors adopting DigiD's ideals of self-mastery helps to carry out the implementation of this new digital technology. Yet, as the state withdraws from the lives of self-governing Dutch residents, it generates its own invisibilization, which is relatively experienced by Dutch residents as a negative effect of the digitalization of bureaucracy.

On the other side of this interface, DigiD further excludes from society Dutch residents from a lower-economic position with no digital competencies – namely, the invisibles. Their lack of digital skills disconnects them from the state as they are unable to communicate with the government. Therefore, this digital form of bureaucracy reproduces the same pre-existing inequalities. Yet, one of the major findings of this research was that DigiD, by exacerbating their exclusion, renders vulnerable people invisible. Vulnerable users are not deemed fit to join digital inclusion programs that posits self-reliant and self-fulfilling individuals as the norm, which reinforces the invisibility of vulnerable DigiD users. Moreover, the invisibles become more dependent rather than self-reliant as they depend on family members or social counselors for the handling of their administration. DigiD, as a form of governmentality, generates the invisibilization of this part of the Dutch society that feels deserted by the state, which they start

trusting less, rendering them, perhaps, even more vulnerable. Finally, this thesis has shown how DigiD does not reduce bureaucracy but rather reinforces it, especially for the invisibles.

Lastly, this study has identified new issues that have emerged with the development of digital bureaucracies. The invisibility of digital bureaucracies renders them difficult to understand by the majority of the Dutch population. Although we tried to shed light on this invisibility, we still cannot fully comprehend the internal functioning of these digital bureaucracies, and that constitutes the second major finding of this research. Digital bureaucracies require an expertise that is only detained by a small part of the population, which was represented by a group of informants that I called "the experts". As the majority of the population lacks sufficient knowledge for understanding digital bureaucracies, it impacts their online security and privacy practices. Dutch residents are urged to ensure their own safety when using their DigiD, yet, they do not perceive any potential threats. The security of Dutch resident's DigiD is predicated upon largely hidden infrastructures, which obscures their understanding of online security, rendering them perhaps even vulnerable to invisible hackers. Finally, this study has found that, generally, Dutch residents do not feel concerned about their data privacy. Yet, I have shown that their indifference was due to their inability to see and relate to their own data. The digitalization of documents, and thereby their invisibilization, has generated a common indifference towards issues of privacy, which is to a certain degree worrisome.

Recommendations for future research

The first limitation of this study is that it lacks some first-hand observations of the invisibles of DigiD's experiences. This study might gain some additional insights if it was repeated by a Dutch-speaker researcher. The second limitation is due to the corona lockdown that was in place during my fieldwork. Future researchers might collect fruitful observations in libraries as they would attend Digisterker courses and experience first-hand how students are progressively being shaped by these empowering digital inclusion programs.

If the debate is to move forward, a better understanding of cybersecurity needs to be developed. It appears that a cross-disciplinary study involving IT experts might shed a greater light onto the invisibility of digital bureaucracies, and thereby provide a better and deeper understanding of these new and obscure infrastructures on which digital forms of bureaucracy now rest. More work needs to be done to understand how security is differently experienced and framed by: the government, the citizens, and by IT experts. From this research, we can already perceive that for the same system, there are different perceptions of security and risks. Therefore further research should focus on determining the impact that these different perceptions can have for the governing of digital bureaucracies and how these different perceptions co-exist in a particular society.

Finally, further research could focus on the experiences of bureaucrats themselves. How have the digitalization of bureaucracy modified their everyday work and, perhaps, their perception of bureaucracy itself? Does the invisibility that DigiD creates render them more indifferent to the lives of citizens? Moreover, a further study could discuss their own invisibility. Indeed, bureaucrats also have become invisible to society, as they are now placed behind a screen. Finally, more work could also determine the impacts that the digitalization of documents also had for bureaucrats. How do bureaucrats experience the loss of materiality, or perhaps, what is that new materiality? Have files and papers completely disappeared from their everyday work ? Or, do bureaucrats still have to deal with documents besides digital files, which maybe also reinforces for them bureaucracy?

Bibliography

Alshehri, Mohammed, and Steve Drew. 2010. "Implementation of e-Government: Advantages and Challenges" *International Journal of Electronic Business* 9(3): 255-270.

Anthony, Denise, Celeste Campos-Castillo, and Christine Horne. 2017. "Toward a sociology of privacy." Annual Review of Sociology 43: 249-269.

Bennett, Colin J., and David Lyon. 2013. *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective*. London: Routledge.

Cody, Francis. 2009. "Inscribing subjects to citizenship: petitions, literacy activism, and the performativity of signature in rural Tamil India." *Cultural Anthropology* 24(3): 347-380.

Dandurand, Guillaume. 2019. "When biopolitics turn digital: transparency, corruption, and erasures from the infrastructure of rationing in Delhi." *PoLAR: Political and Legal Anthropology Review* 42(2): 268-282.

Foucault, Michel. 1991. "Governmentality". In *The Foucault Effect: Studies in Governmentality*, edited by Graham Burchell, Colin Gordon, and Peter Miller, 87-104. University of Chicago, Chicago, US.

Fountain, Jane E. 2001. "The Paradoxes of Public Sector Customer Service." *Governance 14*(1): 55-73.

Fraser, Gary. 2020. "Foucault, governmentality theory and 'neoliberal community development'." *Community Development Journal* 55(3): 437-451.

Goldstein, Daniel M. 2010. "Toward a critical anthropology of security." *Current Anthropology* 51(4): 487-517.

Graeber, David. 2015. *The Utopia of Rules: on Technology, Stupidity, and the Secret Joys of Bureaucracy*. NY: Melville House.

Gupta, Akhil. 2012. *Red Tape: Bureaucracy, Structural Violence, and Poverty in India*. Durham: Duke University Press.

Herzfeld, Michael. 1992. *The Social Production of Indifference: Exploring the Symbolic Roots of Western Democracy*. US: Berg.

Hine, Christine. 2020. *Ethnography for the internet: Embedded, embodied and everyday*. London: Routledge.

Hobbis, Stephanie K., and Geoffrey Hobbis. 2017. “Voter Integrity, Trust and the Promise of Digital Technologies: Biometric Voter Registration in Solomon Islands.” *Anthropological Forum* 27 (2): 114-134.

Hull, Matthew S. 2012. “Documents and bureaucracy.” *Annual Review of Anthropology* 41: 251-267.

Kreiss, Daniel, Megan Finn, and Fred Turner. 2011. “The limits of peer production: some reminders from Marx Weber for the network society.” *New Media & Society* 13(2): 243-259.

Lentzos, Filippa, and Nikolas Rose. 2009. “Governing insecurity: Contingency planning, protection, resilience.” *Economy and Society* 38(2): 230-254.

Lyon, David. 2001. *Surveillance society: Monitoring Everyday Life*. UK: McGraw-Hill Education.

Maguire, Mark. 2009. “The birth of biometric security.” *Anthropology Today* 25(2): 9-14.

Marx, Gary T. 2003. “A Tack in the Shoe: Neutralizing and Resisting.” *Journal of Social Issues* 59(2): 369-390.

Mathur, Nayanika. 2017. “Bureaucracy.” In *The Cambridge Encyclopedia of Anthropology,* edited by Felix Stein, Sian Lazar, Matei Candea, Hildergard Diemberger, Joel Robbins, Andrew Sanchez & Rupert Stasch, 1-12.

Miller, Peter, and Nikolas Rose. 2008. *Governing the Present: Administering Economic, Social and Personal Life*. Cambridge: Polity.

Nuijten, Monique. 2004. “Between fear and fantasy: governmentality and the working of power in Mexico.” *Critique of Anthropology* 24(2): 209-230.

O’Reilly, Karen. 2012. *Ethnographic Methods* (second edition). New York: Routledge.

Park, Sora. 2017. *Digital Capital*. London: Palgrave Macmillan UK.

Rao, Ursula. 2013. “Biometric marginality: UID and the shaping of homeless identities in the city.” *Economic and Political Weekly* 48(13): 71-77.

Rao, Ursula, and Graham Greenleaf. 2013. “Subverting ID from above and below: The uncertain shaping of India's new instrument of e-governance.” *Surveillance & Society* 11(3): 287-300.

Rose, Nikolas. 1993. “Government, authority and expertise in advanced liberalism.” *Economy and Society* 22(3): 283-299.

Rose, Nikolas. 1996. “Governing “advanced” liberal democracies.” In *The Anthropology of the State: A Reader*, 144- 162.

Rose, Nikolas. 1999. *Powers of Freedom: Reframing Political Thought*. Cambridge University Press.

Rose, Nikolas. 2000. “Government and control.” *British journal of criminology* 40(2): 321-339.

Rose, Nikolas. 2006. “Governing ‘Advanced’ Liberal Democracies” In *The anthropology of the state: a reader*, edited by Aradhana Sharma and Akhil Gupta, 144-162. UK: Blackwell Publishing.

Sharma, Aradhana, and Akhil Gupta, eds. 2006. “Introduction: Rethinking Theories of the State in an Age of Globalization.” In *The anthropology of the state: a reader*. UK: Blackwell Publishing.

Viseu, Ana, Andrew Clement, and Jane Aspinall. 2004. “Situating privacy online: Complex perceptions and everyday practices.” *Information, Communication & Society* 7(1): 92-114.

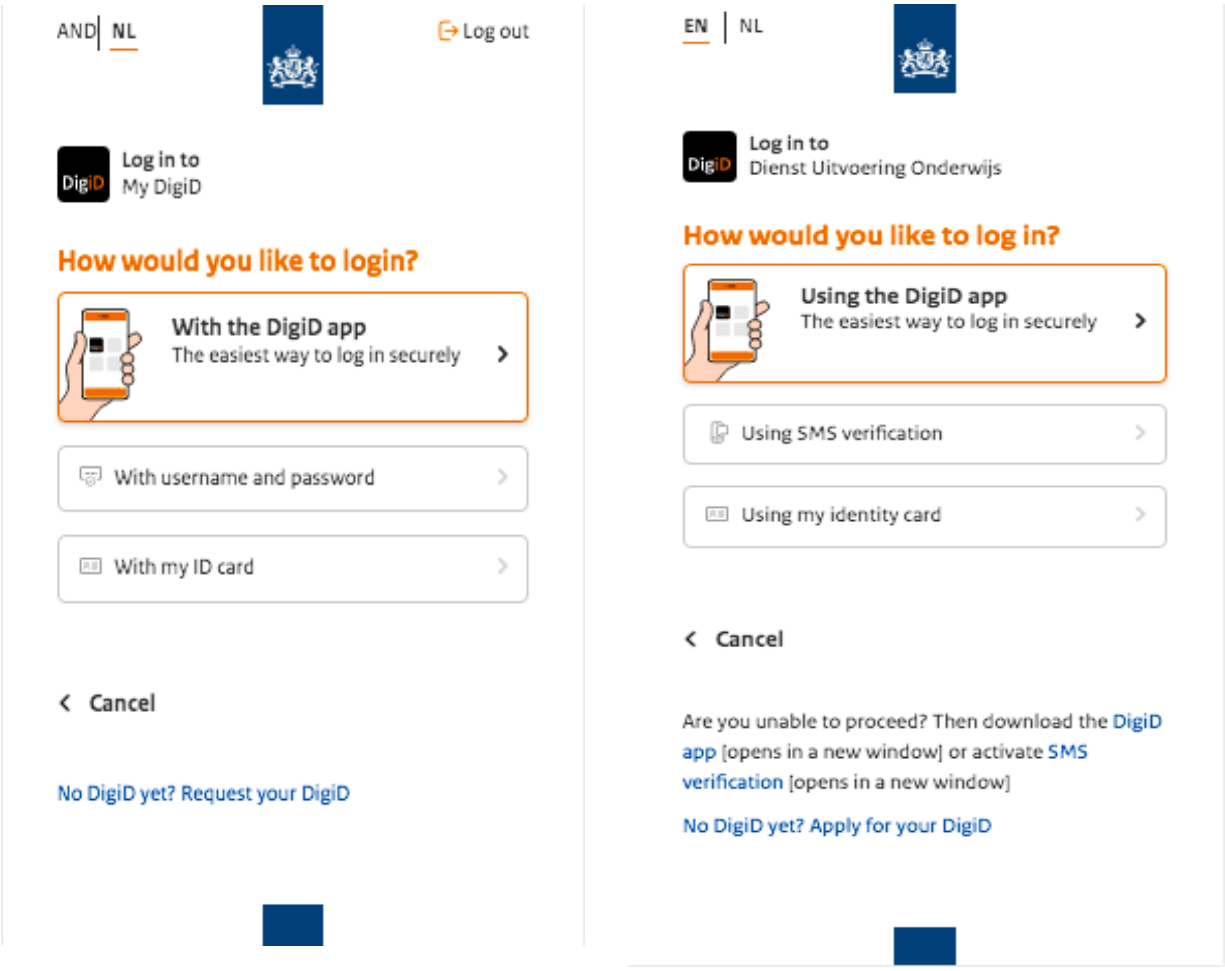
Woolward, Marc. 2017. “Risk-based approaches to cybersecurity.” *Risk Management* 64(5): 8-9.

Weber, Max. (1922) 2019. *Economy and Society*. Harvard University Press.

Whitfield, Dexter. 2012. *In Place of Austerity: Reconstructing the economy, state and public services*. UK: Spokesman Books.

Appendices A – Different perspectives of the login process

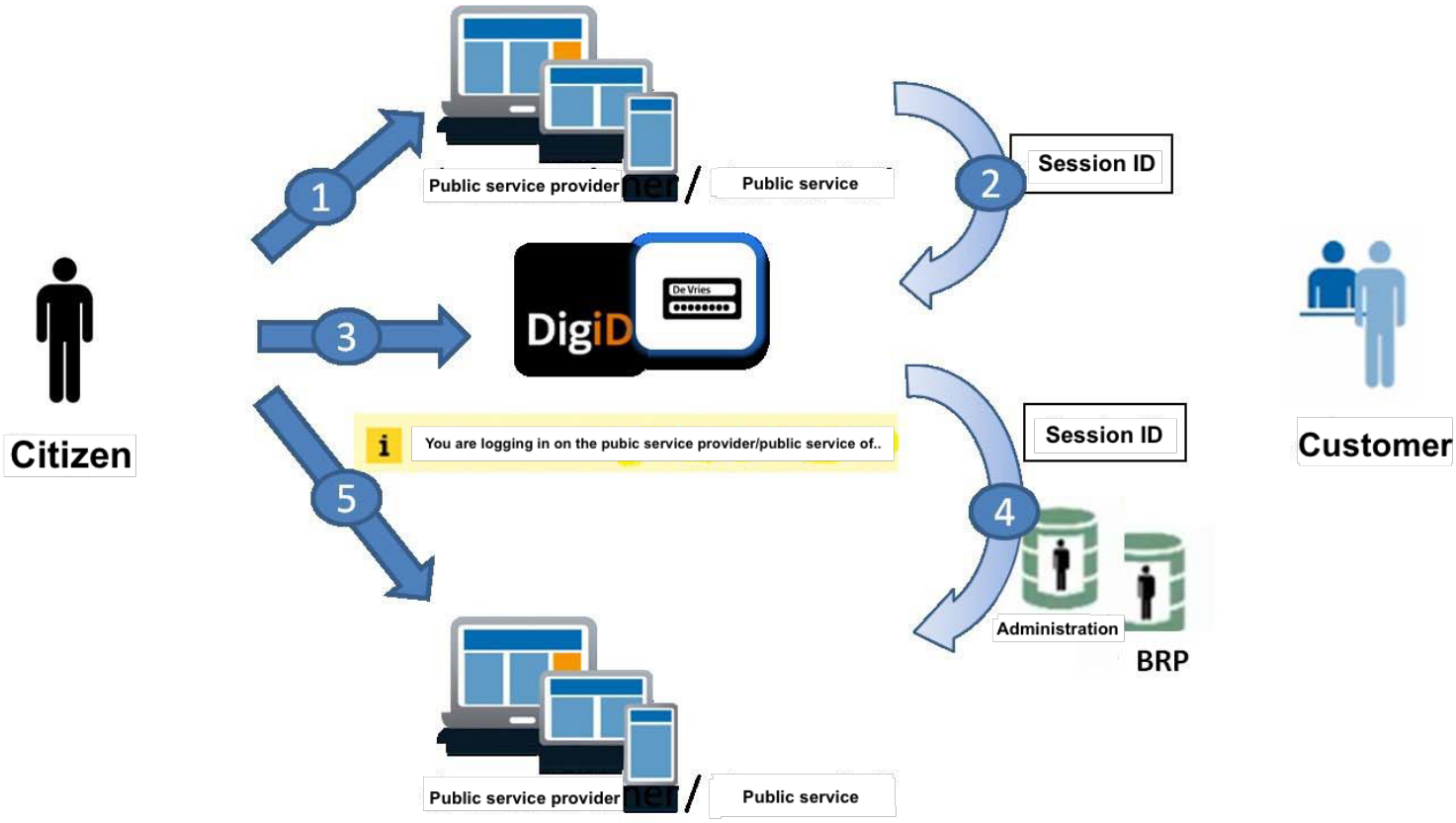
A.1. From the user's perspective



Source:

https://www.logius.nl/diensten/digid/documentatie/functionele-beschrijving-digid#hoe-werkt-authentiseren-gebruikersperspectief, accessed August 7, 2021.

A.2. From the organization's perspective



Source:

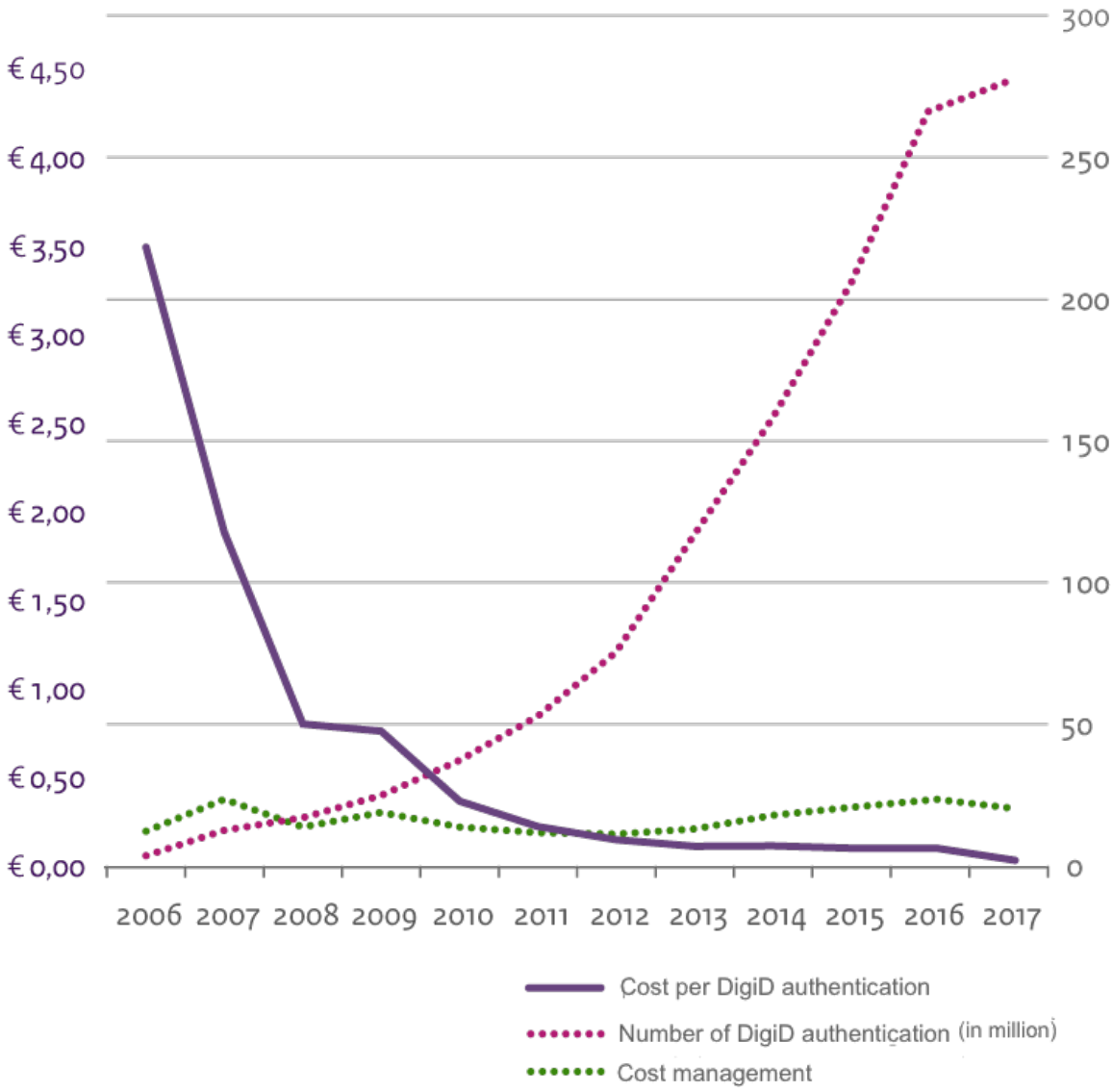
https://www.logius.nl/diensten/digid/documentatie/functionele-beschrijving-digid#hoe-werkt-authentiseren-gebruikersperspectief, accessed August 7, 2021.

A.3. From Logius' perspective

Source:

https://www.logius.nl/diensten/digid/documentatie/functionele-beschrijving-digid#hoe-werkt-authentiseren-gebruikersperspectief, accessed August 7, 2021.

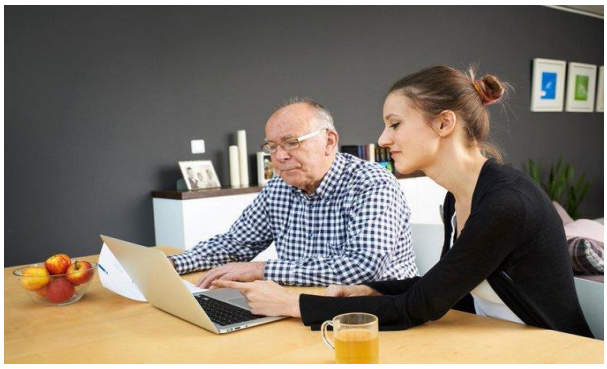
Appendices B – Chart of the evolution of the costs and numbers of DigiD authentication



Source:

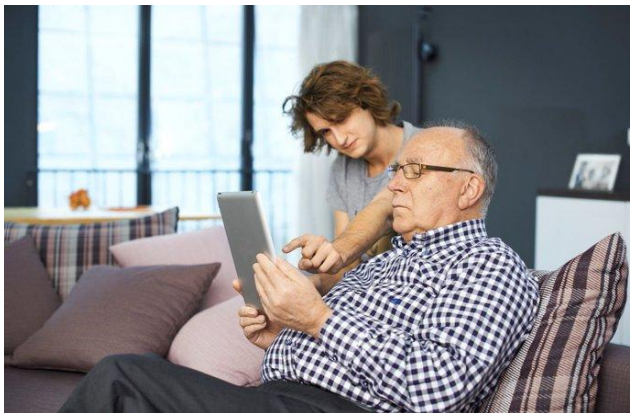
https://magazines.logius.nl/logiusjaarverslag/2017/01/financien, accessed August 7, 2021.

Appendices C – Pictures posted on the Twitter account @DigiDwebcare



Posted on the 17th of February 2021.

Source: https://twitter.com/DigiDwebcare/status/1362070286707916804/photo/1, accessed August 9, 2021.



Posted on the 18th of February 2021

Source: https://twitter.com/DigiDwebcare/status/1362432704470466561/photo/1, accessed August 9, 2021.

Posted on the 25th of February 2021

Source: https://twitter.com/DigiDwebcare/status/1364863950618320896/photo/1, accessed August 9, 2021.

Appendices D – Questions of the online Digitest

1. **What is probably the correct internet address of Digisterker?**

    - http://www.digisterker@nl
    - http://wwwdigisterker.nl
    - http://www.digisterker.nl
    - None of all three

2. **Where can you find the internet addresses that you have saved?**

    - Explorer
    - Favorites
    - History
    - In all three places

3. **How can you view the bottom of a web page when it doesn't fit in the window?**

    - Double click on the tab
    - Drag the slider down
    - Click at the bottom of the window
    - None all of three

4. **How can you recognize a link or hyperlink on a web page?**

    - By the little hand that appears when you place the pointer over it
    - By the color: a link or hyperlink is always blue
    - To the form: a link or hyperlink is always a button

5. **Do you have to enter http:// for each internet address?**

    - Yes
    - No

6. **What are cookies?**

    - Programs installed on your computer while browsing
    - Small text files that are stored on your computer while surfing
    - None of all three

7. **What does a green padlock mean for a web address?**

    - This webpage has been locked because it is unsafe
    - It is better not to enter any personal information here
    - You are in a secure area
    - All three are correct

8. **What is iDEAL?**

    - A fast and secure payment method for online purchases
    - A program to protect your computer from spyware
    - A method to secretly find out your financial data
    - None of all three

9. **You have ordered a book via the Internet and paid directly via iDEAL. How do you know that the order has also arrived at the online bookstore?**

    - It's a matter of trust, you won't know until the book arrives
    - The supplier and iDEAL will send a confirmation e-mail
    - You will receive an invoice from the online bookstore

10. **Does an e-mail address always contain the @ symbol?**

    - Yes
    - No

Source:

https://fd7.formdesk.com/oostachterhoek/digitest/?get=1&sidn=bbe7d585922e4ffa9b74517e02dc5173, accessed August 7, 2021.

Appendices E – Screenshot of the list of Logius' IT suppliers

Suppliers AF	Suppliers GZ
4Value	ShireIT
Anoigo Services	Green Valley
Arpha	GX Software
atos	Idella-Visma
BakerWare	Indicia
Brain	Info projects
CARE internet services	Mirabeau
centric	Mozart
Circle Software	Muse
colors	onegini
CSC	PinkRocade
Vigor	Seneca
Data B Mail service	Signicat
Decos	SIM group
Enable-U	TamTam
eConnections	TOG Netherlands
Excellence	Traxion
EzCompany	TrueLime
funatic	VitaHealth Software
MunicipalitySolutions	WIND Internet
Gino	YourRequest
	Zaaksysteem.nl

Source:

https://www.logius.nl/diensten/digid/ict-leveranciers-digid, accessed August 7, 2021.