Function Creep in Surveillance Situations

Identifying control paradoxes through agency and power relations using ANT

Manon Jacobs

3939901

New Media & Digital Culture

Master thesis

Hand-in date 21-06-2016

Supervisor: Ingrid Hoofd

Abstract

In this thesis, I research the manner in which function creeps come to exist in surveillance situations, and how we may recognize them in future situations. Additionally, the ambiguous nature of function creeps is discussed. Finally, I will argue that function creeps are the product of a type of control paradox, where the agency of the ICTs used in surveillance situations leads to surveillers (both businesses and governments) taking more risks and through this, potentially disrupting their original goal. I utilize ANT and surveillance theories to provide a framework for my analyses, which consist of four case studies: two potential function creep situations, and two known function creep situations.

Contents

Introduction

Data collection can happen on all levels of our daily lives. Recently, car manufacturers like Tesla and GM have been starting to combine the collection of data through ‘black boxes’ in consumer vehicles to increase safety. Tesla vehicles can intervene when an accident is about to happen, adjusting speed or even direction. This data, in addition to providing a safer driving experience, could prove fruitful for future business opportunities. The collection of vehicle data, even through using crude black boxes in the past, have shown to make roads safer (NHTSA, 2001). Opportunities following the collection of this data are increasing: this data could be used in law enforcement, and in the insurance business. In the future, these changes in the use of the data will be implemented, and as early as 2020, 90% of cars will have this technology implemented, says Tom Simonite of MIT Technology Review (2016). Slow changes to these technologies alter the way in which they work, and add dimensions to products that we use that may not be focused on improving the user experience, but instead allow a company go make their product (more) profitable. Now that we as a society are used to technology enhancing our lives, and making our lives easier, it seems that we are willing to part with almost as much privacy as the companies backing the products we use, ask us (Davidson, 2014). These changing relationships between technology, the organizations employing the technology, and the end subjects, often consumers, are the subject of this thesis. We will be touching upon different kinds of surveillance practiced by governments and for-profit firms alike, as well as the way in which this surveillance ‘creeps’ into the expanded use of technologies.

This will be achieved through the use of Actor Network Theory, and three separate case studies.
The following are the inducement and the leading factors in this research. They are as follows:

Main argument
My main argument in this thesis is that when *function creeps* occur in surveillance situations, they are created by a kind of ‘control paradox’ through the power imbalance that leads up to the function creep. By ‘control paradox’ I refer to what happens when a person (or organization) acts a certain way to achieve a particular goal, but through the actions taken, they may actually undermine their own efforts. Further explanation on this subject in chapter one, **page 7.**

In addition, I propose that:

1. We can recognize future function creep cases by examining 'known' and 'potential' cases by following the power relationships occurring in the actor networks that make up these function creep situations;
2. Function creep is a natural occurrence in our technology driven consumer culture, and has ambiguous consequences.

I will be focusing on function creep occurring in surveillance situations, in both governmental and for-profit organizations. There are four cases I will be examining. I will begin with two 'potential' function creep cases. The first is the Chinese government's plan for implementing a so-called Social Credit System. The second of the potential function creeps is the planned use of monitoring technology in exchange for lower insurance premiums by Dutch insurance group Achmea. Following these 'potential' cases, I will move on to the 'known' function creep cases. The first of these two cases revolves around the application of the United Kingdom's sex offender register. Lastly, I will be researching the occurrence of function creep in the utilization of biometric data in Dutch civilian passports.

Function Creep

The situations in which function creep occurs, are the outcome of our current society, where often fear of terrorism influences governments and their officials into creating measures that are meant to improve security, but also, often after a while, 'creep' into a citizen controlling tool (Saetnan, Lomell & Wiecek, p. 408 & Maurits, 2013). The definition of function creep I will be using in context of this thesis and the cases above, is as follows:

Oftentimes only used in a very negative sense, function creep is often a consequence of perpetuated fear of, for example, terrorist acts, and the responses Western governments have created in the form of regulations and laws. In addition, as we will be seeing with our first case, function creep may also come forth in the surveillance that is put into place because of a want for harmony of an entire country, as in the case of the Chinese government's plan. Function creep also occurs when businesses are confronted with opportunities to increase income, through collecting and using consumer data.

All of the cases we will be investigating fit the above profile, and we will be focusing on the agency and the power relations that it creates between different actants within these networks to research how function creep occurs.

Motivation for this research

The idea of function creep shows that we, as a society, lose control of technology when it is allocated for a different function. The purpose of a particular designed technology shifts when a person or institution with the power to influence the function of a technology decides that a technology's efforts should be directed elsewhere; effectively adding functions. The phenomenon function creep reveals that the power associated with the use of a technology can shift over time, from either a person/institution to another, or a change in goals for a technology. This lies at the basis of the motivation to perform this research; the power inherent in technologies is associated with the wielder of that technology, and his intentions. If that technology is pointed at accumulating as much data as possible on individuals, these individuals' privacy is reduced to what they choose to try and hide from these technologies. That is the agency users of smart technology have; the data we envelop ourselves with, the information we share on smart devices and social media. David Lyon emphasizes that in surveillance, power is intrinsic. Surveillance is put in place by an authority to care for, control or influence people (2003, p. 3).

In society, and in news media[1] most kinds of surveillance are typed as invasive and intrusive: Lyon (2003) says that social relations and social power are partly organized by surveillance (p.4). An argument to support this can be made with Foucault's example of a Panopticon. The subjects under the surveillance of the Panopticon are not aware when or if they are being watched, leaving the control with the watchers. This control can seen in the control felt by consumers when they trust (online) services with their personal information. Consumers and citizens have been giving their right to privacy in exchange for safety, or convenience. In a 2014 survey, users of online services were asked whether they prepared to trade privacy for greater convenience (Lohr, 2014). Over half of respondents in the US and the UK said 'no'. However, seeing as the amount information shared by users is only increasing, it seems to indicate the opposite. Businesses consumers trust everyday, as well as governments aiming to increase public safety worldwide, might just have our best interests at heart. However, many civil rights groups and privacy focused organizations fight for consumers' rights to retain their privacies[2]. When does surveillance turn from protection and convenience into a Bad Thing? Should we halt the process of the sharing of personal information online and to institutions and governments? Instances of Function Creep have privacy rights organizations and like-minded individuals saying 'Yes', (Zenger, 2012) since organizations are repurposing data and technology they control. Articles on the function creep are often written in a tone resembling 'What can we do to stop this?' (Zenger, 2012), while we may want to focus more on what particular instances of surveillance result in, and how they are created.

[1] An example; the New York times has a continuous topic devoted to 'Surveillance of Citizens by Government' in which every news story on this topic is arrayed. The lion's share of these news stories has negative connotations regarding the invasiveness of surveillance, and the privacy and ethical concerns plaguing the use of surveillance. Access to NYTimes topic: http://www.nytimes.com/topic/subject/surveillance-of-citizens-by-government

[2] These include many, such as international NGOs: Privacy International, EPIC, the Electronic Frontier Foundation, and local initiatives such as the Dutch Bits of Freedom.

Actor Network Theory in this research

“Theories usually try to explain why something happens, but actor-network theory is descriptive rather than foundational in explanatory terms, (...) it tells stories about ‘how’ relations assemble or don’t” - (Law, 2007, p. 3)

Actor Network Theory has been selected as the method for researching Function Creep, in the different case studies chosen for this research. ANT will be employed to lay out and investigate the different relationships between human and non-human actors in selected situations. For this research, I will be focusing on the different power relations between human and non-human actants. Four case studies will be undertaken, of which two are ‘known’ function creeps in practice, and the other two have been marked as ‘potential’ cases of function creep. The goal is to accurately describe the heterogeneous systems that are inherent to the case studies; identifying possible control paradoxes and examining the research statements made on page 4. More on the use of Actor Network Theory in this research in chapter four.

The structure of this thesis

Firstly, the current academic discussion on privacy and surveillance will be elaborated on in chapter one. Next, we will be touching upon technological artifacts and their potential agencies in chapter two. Then, to explain further the use of ANT in this thesis, chapter three will provide the basis for the case study analyses that will be expanded upon in chapter four. To conclude, I will discuss my findings from these analyses in chapter five.

1. Privacy and surveillance: A multifaceted discussion

To further define the different elements that make up the subject of this thesis, I will first discuss the use of surveillance, and the, almost always directly related, issue of privacy. In all four of the case studies that will be examined in this research, the privacy concerns of those under scrutiny is an important factor in deciding whether the negative consequences outweigh the positive (or vice versa) in function creep in surveillance situations (see hypothesis two in the introduction).

The subjects privacy and surveillance are intertwined at many points. It is the surveillance of organisations (and, sometimes, the 'sousveillance' of our fellow citizens) that impacts our sense of privacy. Directly related to our *sense* of privacy, is our *right* to privacy. Society generally feels that an individual's right to lead a life in which personal information is protected, is of varying importance (Whitman, 2004); when an individual (or a group) is deemed potentially dangerous, the subject switches to a comparison between how many rights someone with, for example, a criminal past, still ought to have, and how much of a threat a person or group poses if we do not investigate their personal affairs. David Lyon (2003) poses that surveillance is not merely a matter of the impact it makes on personal privacy, but that it is also a matter of creating and keeping long term social differences, in a process he calls 'social sorting'. In this process, he says, individuals are assigned worth or risk, depending on their personal characteristics. This idea is not entirely new; Oscar Gandy (1993) spoke of the manner in which transaction data was used to target individuals for advertisements, and ignore others.

Surveillance causes people to be categorized through their spending habits, but also their culture, such as the profiling that occurs at, for example, American border security checkpoints. These practices became more common on US soil after the 9/11 attacks (Chisti & Bergaron, 2011). In 2014, the Obama administration reaffirmed the practice of profiling based on religion and country of origin at border control (Howell, 2014). Although the practices of profiling and mapping (using demographic data to target neighbourhoods) were continued after a new policy rollout in 2014, many in-field agents and officials feel that the new rules limit their professional efficacy. However, the fact of that the FBI is allowed to continue their practices in identifying persons and areas of interests solely based on demographics, has democratic lawmakers and civil rights groups saying that there is still a long way to go (Horwitz & Markon, 2014). Of course, surveillance is the only way in which security agencies in North America and other countries can reliably keep an eye on what they believe are dangerous individuals. However, many believe that the human subjectivity involved makes these sensitive measures vulnerable to error and prejudices (Horwitz & Markon, 2014).

The use of surveillance often serves one or both of two goals; the gathering of personal data for economic gain, and to increase security, in many kinds of situations. We have briefly discussed both in the paragraphs above. With regards to surveillance serving security problems, many organizations and governments have to balance whether the end justifies the means. Is it worth gaining a sense of safety by knowing where certain people are, against breaking those people's rights to privacy? Nick Taylor (2002, p.66), professor of Law points out that for citizens to accept and support public surveillance, the surveillers have to be kept accountable. This balance is potentially fragile: if a situation were to be affected by function creep, the balance between earnings or safety to be gained and right to privacy could be skewed. This can be related to a type of control paradox: the more an organization attains additional functions (such as perhaps the safety and wellbeing of citizens) through increased surveillance, this could potentially push the privacies of the people surveilled to an area of lesser importance. Of course, in for-profit situations the privacy of consumers is not of primary concern to companies. However, often it is stated in the planning (such as a company statement, or press release) surrounding potential function creeps in commercial situations that personal privacy of customers is of high concern. Not keeping their own word through the effects of function creep and this control paradox could hurt businesses in the end. The term control paradox has been used in the context of privacy in the past: in 2013, researchers Brandimarte, Acquisti and Loewenstein looked into what they called the control paradox in how the increase of an individual perceived control over the release and access of private information also increased their willingness to share such information. They explain that the paradox of control is centered around the *feeling* of being in control, and the directly associated increase in the willingness to take risks[3] (Brandimarte, Acquistie & Loewenstein, p. 340). Using technology that allows a business or government to further increase surveillance fuels the feeling of being in control, however, this increase, this risk-taking, might actually have the reverse effect of the goals set in the first place.

At what point does the end no longer the means? Harris et al. (1995, p. 297) mention that the use of surveillance can be seen as action against any crime, between a parking violation and a homicide. The weight of these crimes, of course, differs, however, any violation of citizens' rights would occur on the same level. This is important to consider in this research, since we will be examining both negative and positive consequences of function creep occurring in these types of surveillance situations. Striking a balance between privacy concern and the pursuits of profit or security may create this same balance, halting control paradox situations and preventing function creep.

The discussion of privacy in criminal justice in the US has had the following point of view since the 1970s, Taylor (p. 75) says: "(...) the test of privacy was not dependant wholly on location but where one would have a 'reasonable expectation of privacy'". An interesting point, especially when looking at the, what some call, breaches in privacy by for-profit organizations. Personal data such as spending patterns and people's

[3] Risk perception and risk taking are both determined by control, say the following researchers: Weinstein, 1984; Slovic, 1987; Harris, 1996; Klein & Kunda, 1994 and Nordgren, Van der Pligt, & Van Harreveld, 2007.

interests are high in value for (tech) companies. These are companies such as Google and Facebook, that continually analyze the content their users feed them. Even if a person is not a Gmail user, merely sending an email to someone with such an account will have Google analyze the message word by word:

> *Our automated systems analyze your content (including e-mails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored.*
>
> Source: Google Terms of Service[4]

It is interesting to note that while the Electronic Frontier Foundation sued the US government on citizens' behalfs over the FBI's facial recognition systems (Lynch, J. 2014), companies like Google and Facebook continue to profit from the personal data shared by users, and people gladly continue to partake in their services. According to a 2014 survey which showed that while people may *say* that they value their privacy over the use of social media and the convenience of services such as Gmail, this is not reflected by their behavior (Davidson, 2014). The people surveyed were asked whether they would be willing to trade their personal information for more convenient online experiences; 51% replied 'no', and 27% said 'yes' (all others were unsure or did not have an opinion on the matter) (EMC, 2014). In addition, the largest part of the respondents also said that they were of the opinion that "businesses using, trading or selling my personal data for financial gain without my knowledge or benefit" were the largest threat against their personal privacy (EMC, 2014). These results seem to be bad news for companies like Facebook and Google who rely on this information. However, these results did not hurt Google's business in the least, growing bigger every year since (Dougherty, 2016).

The reliance on products that are presented to consumers by companies we know and choose to trust result in the agency of these products over us to grow. So how does this work? What role does technology play in the power struggle surrounding surveillance situations? The following chapter will answer these questions.

[4] Retrieved from: https://www.google.com/policies/terms/

2. Technological artifacts and their associated power

“(...) power relations are intrinsic to surveillance processes” - D. Lyon, 2010

Surveillance, whether it is practiced by authorities or companies, is enabled through the same information technologies. These ICTs (Information and Communication Technologies) are difficult to regulate, since new developments arise continually, and legislation takes time, says David Lyon (2010, p. 2). A saying comes to mind, as popularized in modern times by the comic ‘Spider-Man’[5]: “With great power, comes great responsibility.” Surveillance grants such power, an example of this is the panopticon, as used by Foucault in his writings: a circular building that features a single centered watchtower, which has the effect that the inmates never know whether they are being watched. The permanent visibility creates the situation in which these inmates are continuously under control of the watchers.

In today’s society, this panopticon is embodied by both CCTV systems in hands of law enforcement, and the accumulation of data in online services. In profit-driven organisations, the goal of data accumulation is reached by designing applications and media that invite, and require to a certain point, the sharing of personal information by their users. Both the CCTV system and the applications/media platforms have power over the people who are either willingly, or unwillingly, interacting with them. These systems are made up of technological *artifacts*; items invented by humans to solve problems. This use of technology provides governments and organisations with enormous capabilities in terms of surveillance: they are empowered by the technological solutions they employ for their goals.

It has been established in the previous chapter that the power of surveillance technologies such as CCTV through the panopticon theory supports its effectivity in how visible surveillance technologies are a two edged sword. However, we have not yet discussed how ICTs are used to increase the reach, power and capacity of online surveillance systems. These systems are focused on processing personal data for diverse purposes: from caring and managing, to influencing and controlling both individuals and entire populations (Lyon, 2010, p.110). There are obvious surveillance situations, such as when an individual is ‘screened’ before boarding a flight at an airport. That is the first reason for organizations to use surveillance; immigration departments want to know who leaves and enters their country. Secondly, commercial data is

[5] In the comic, the quote is uttered by Ben Parker, uncle to Peter Parker (Spider-Man). Amazing Fantasy #15, 1962.

processed by private organizations, such as the airline used by the travellers. This data is important to these companies because it provides information on who flies where and when.

David Lyon (2010, p. 111) sees all of these kinds of surveillance situations (for security, and also commercial reasons) as occasions in which we are ‘individuated’: “distinguished from others, identified” and “assigned worth or risk”. This happens through the particular criteria set by the organization doing the surveilling, followed by an analysis of our behavior, communication or transaction is initiated, Lyon (2010, p. 111) says. People are divided and categorized through their purchasing behaviors, and through this, social power and relations are organized partly through surveillance. This categorization may be either disrupted or expanded through function creep occurring to these practices.

Data is the resource to be mined in the 21st century. To mine this resource, especially in larger quantities, devices with these capabilities enter our lives at perhaps unexpected points. More and more (household) technologies are becoming ‘smart’, making users’ lives more convenient, while also providing those same users’ information to the companies behind these devices. Commonly referred to as ‘the Internet of Things’ (IoT), this involves all things that are embedded with technology and that people come into contact with throughout their daily lives. The ‘things’ referred to in IoT can be a wide variety of instruments, from biochips in farm animals, to cars with built-in sensors, to heart monitoring implants, to refrigerators. Technology and advisory corporation Gartner, Inc. (2013) predicts that by 2020, as many as twenty-six billion devices will be linked by IoT. This Internet of Things creates the opportunity to collect and analyse an accumulating amount of behavioural information. The Guardian’s Angie Moss (2014) predicts that the cross-correlation of all of the devices’ data could potentially revolutionise the targeted marketing of products and services, since Function creep occurring in surveillance in the future might have more far reaching consequences than they do now, with today’s technologies, because of the emergence of the IoT. This is why it is vital that we search for a way through which we may identify future potential function creep situations. To find this, we must first investigate currently planned potential cases, and past cases.

3. Using Actor Network Theory in this research

It is difficult to say that Actor Network Theory is the ‘methodology’ of this research into function creep. This thesis will mobilize ANT, weaving in into surveillance theory, structuring the analysis the case studies in chapter four. ANT, as introduced by Michel Callon, John Law, and Bruno Latour in 1977, is actually not straight-forwardly a method. Rather, it is a theory in which to place human and non-human actors, and the ever-changing relations between them. These relations, connected as such in that they form a network, are key in researching the distribution and (im)balances in power resulting in function creep situations. ANT provides us with a description of how the connection between entities, both human and non-human, may lead to the formulation of new entities. Latour shows this in his 1999 essay Pandora’s Hope. In it, he describes the situation of how a third entity is created when a man and a gun are directly connected. This third entity is the gunman. The weapon without the man is an object that does not move, or kill, on its own: it is the sum of the two parts that make the gunman. If we would be able to break the connections between the man and the gun, the existence of both men and guns would not give us any problems anymore. ANT looks to have the researcher investigate the connection between the man and the gun. With this example, Latour shows us that the connection between two different entities (actors, actants) may create new entities that are not a mere sum of the original entities’ characteristics. For example, a man and a gun could indeed be a man merely holding the gun. However, there is also the (perhaps) dangerous possibility of the gunman. Through the focus on connections, we can conclude that ANT is a constructivist theory; observing the context in the relations between the actors. The ‘Actor’ part of ANT may lead to some thinking that ANT is focused on human interactions. However, as we were able to see through the gunman example, the gun is as much part of the equation as the man ever was.

The actors in ANT are any entity, collective or individual, that can associate or disassociate with other entities. Even though ‘actor’ is in the name of the theory, it is not used in the analyses following the theory. Instead, the name ‘actant’ is used, since this allows for not only humans, but also animals and objects to be included. The definition of an actant in Greimas et al.’s Semiotics dictionary, is as follows: “ An actant is that which accomplishes or undergoes a certain act”, and this is exactly how we may see actants in ANT. It is when actants enter into networked contact which provides them with “substance, action, intention, and subjectivity” (Ritzer, 2004). Ritzer goes on to explain that this means that the actants in ANT are considered undetermined by nature, with no essence of their own, and that it is only through their networks that they may derive their nature: the gunman was only a gunman after the needed comprising actants were connected.

To be able to use ANT practically in this research, we may follow the lead of French sociologist Michel Callon, expert on ANT. Callon describes four stages in using ANT in research in his paper on French scallops (1984). Callon describes “the four moments of translation”, following actants through the construction and deconstruction of a network (1984, p. 59). There is *problematization,* in which the ‘problem’ and situation is identified, in addition to the introduction of the involved actants. The actants defined here, within the network, by the related actants; their ‘wants’ lies at the foundation of their identities. The second stage is *interessement* in which the problematization actually takes place. The different actants act on their wants, and the network comes into being; as Callon calls it, “how they are locked into place” (p 61). In this, the actant employs actions to start influencing other actants in the network, this is the agency of an actant, which will be discussed on the next page. The third ‘moment’ is *enrollment*. The influencing of other actants (interessement) does not automatically lead to a successful network, until enrollment is achieved (Callon, p. 65). The actants in the network have to work together, enrolling in a specific communal situation, in order for the network to stabilize. This leads to the network to function, meaning that the first three stages have led to the network being created. The fourth and last stage is the *mobilization* stage. This is when the actants in the created network have actually started interacting, towards the common cause, the situation that was identified in the first problematization fase. Callon explains that even though these phases are presented as being separate moments, they instead happen simultaneously in reality (p.66). Callon’s four phases will be held as framework for the analysis chapter, in which the power relations will be followed to investigate the creation of function creep situations.

In addition to Callon’s framework, there are additional important concepts inherent to using ANT in research, called ‘punctualization’ and ‘depunctualization’. First described in Latour’s Pandora’s Hope (1999), these terms revolve around the way in which we may dive deeper into particular actants. To illustrate, an example: Two cars crash into each other at an intersection. These cars colliding have at least 4 major actants: the two drivers, and the two cars. If one of the cars was malfunctioning, and through that, caused the accident, one would have to include the broken component as an actant. Indeed, without that particular component misbehaving and changing the other actants, the accident would not have occurred. The deconstruction of the car to include the component in the actor network is called depunctualization. As soon as one thinks of the specific elements that converge to make a car, depunctualisation is achieved. Latour shows us this in Pandora’s Hope (1999), and likens the punctualization of intricate structures, whether it be a building, or vehicle, to a black box. When it is ‘opened’ for further investigation, depunctualisation takes place. In the analysis of the networks involving function creep, it is very much possible that through depunctialisation, we may locate the specific powerful parts of actants.

For every actor network analysis, a single truth can be found: the essences of actor networks are derived from connection, disconnection, and reconnection of their parts (Law, 1992, p.385). An actant without a network exists, but lacks essence. The interaction between different actants provides context, and allocates

power, in the enrollment phase. Through this, we may see that in certain networks, a piece of technology such as a videocamera also derives its meaning through the network it occupies. An example is the video camera: a useful tool to use in creating memories of important events. In that instance, a particular network could consist of the video camera, the subject (perhaps a recently graduated student) and the person using the camera, maybe a parent looking to capture the moment in a homevideo. The power intrinsic to this network is an emotional one; a moment of great importance to all humans involved, and the camera enables the human in this network to create virtual keepsakes. Let us now look at a different network the camera may find itself in. The same type of camera, connected to different, other actants. The user, a volunteer turned whistleblower in the refugee crisis, is one of the present actants, while the others are unaware of their position in this network, much like many human actants are in large scale networks. These last actants are people fleeing their country, arriving in Greece, looking for a safe harbor.
These are completely different situations, different networks, both with different powers emanating from the connections between the actants. A result from the last actor network could be that the video made was shared on the Internet, creating awareness, and moving others to action; powerful outcomes from a similar network to the first.

This power to change other actants in a network, is called agency. John Law (1992) wrote “Interaction is all that there is” (p.379): it is that same interaction that lets one actor influence others, and vice versa. This influence also leads to change, which leads to the network itself changing: perpetual interaction and change. ANT shows us that it is not only humans that influence constantly, as the examples above have shown. Agency is also the case for the non-human actants - an example could be the agency a television has in a bar: when facing the television, some people ‘must’ watch, even though they may consciously not even want to. A mobile phone running out of battery can make many people often desperate. These are small ways in which the agency of these non-human actants influences and changes us, in both behavior and emotional state. In turn, humans can influence these non-human actants as well; you can ask the bartender to turn off the television in the bar, and you can charge your phone to have it regain its battery charge. In the case of function creep, which will be thoroughly researched in the coming chapters, this interaction between actants is as much between both human and non-human actants as it is in other networks. An example of a possible function creep actor network, with both human and non-human actants, is the following: A hospital is seeking to introduce all-digital patient files. The introduction of this system will save time through digital filing, and patients may look into their files whenever they please. Function creep could occur if the hospital administrators would be tempted to use the digital personal data they now have for another goal than health care. They may want to use this data in leverage with insurance companies. The different agencies of each actant, depunctualized or not, will have to be examined and charted. Inside these networks, actants influence and change the other actants. Computers and related systems allow this hospital to collect the data. Their affordance to the hospital administration is the data collection. To Latour, power is not some essence that can be obtained. It is the outcome of the combination, the networking, of multiple actants. The computer by itself is a ‘mere’ calculator. Networked with a human actor, however, they influence one another, and *empower* each other.

In conclusion, the choice for ANT (in combination with surveillance theories) was made because it allows to view networks in a way that considers of power relations as an occurrence within the process of making and remaking of networks, and as such avoiding a reification of power (Law, 2009, p.145). In addition, ANT allows for a description of networks without going too in-depth into the relations between actants (Law 2009). As we have seen above, it also allows for the inclusion of actants that themselves do not have a voice, most probably non-human actants. When linked with surveillance theories, I will be able to specifically research the power relations in the following function creep case studies, while also placing the cases in the framework set by chapter 1, on surveillance and privacy.

4. ANT & Surveillance: Function Creep case studies

In this chapter, we will be looking at how networks in surveillance situations come into existence, and create and endow actants with agency, which in turn cause power relations to occur between actants. In addition, we will be examining these cases to see whether we can discover a common profile for function creep occuring in surveillance situations. The reason for this research to be looking at the power relations involved specifically, is because of how it shapes situations and networks. From following the distribution of power - from both human and non-human actants - I will be specifying the manner in which these function creeps are brought into existence. Following each analysis, I will evaluate the networks leading up and into the function creeps, identifying possible paradoxes of control. In addition, I will be coupling surveillance theories specified in chapter 1 (such as the works of Harris et al, Taylor, and Lyon) to assess each case study rigorously.

If we were to take function creeps as an entire phenomenon, and unleash ANT on that, it would be a task without end. This is because one can delve as deep as they want through depunctualization, and since all networks are exist through their own construction and deconstruction, a researcher could hypothetically delve as deep as they want. To keep this task manageable, I will limit myself to the following four case studies, and will only be focusing on the particular context in which function creep occurs.

Firstly, the two categories touched upon in the introduction of this thesis will be addressed: we will look at possible function creep situations, and function creeps that have been identified as such before. The ‘known’ function creeps are how biometric data was treated with regards to Dutch passports, and the sex offender register used in the United Kingdom. From these situations, we were able to learn what a function creep entails, and what the elements are that we may recognize in other situations. Also, the effects of the potential control paradoxes will be evaluated.
Starting with the most obvious, it is the ‘breaching’ of the extent to what a company or government has declared they will do. Additionally, it is the ‘creeping in’ of another function that was not there before, and which was most often not expected by the public or the subjects of the surveillance, since it was not announced. I refer to the introduction of this thesis for the full definition of function creep that I use.

The ‘potential’ function creep cases are the Chinese Social Credit System, and Achmea’s plan for reducing client payment in return for information on their home and car; we will be assessing the flow of power and agency in these situations, which we will then be able to compare to the ‘known’ function creeps, to establish a manner through which we may be able to identify potential future function creep situations.

4.1 ‘Potential’ Function Creep cases

4.1.1 China’s SCS

The Chinese Social Credit System is an ambitious undertaking. It seeks to ‘rate’ all citizens with scores on how well they perform in various parts of their lives. For example, a person who actively helps other citizens with voluntary activities will receive points for this. Performing well at your job will assure you of a good score, as well as having good credit and paying your bills on time. The system has not been implemented as of this writing; for now, the government is conducting an experiment in how eight Chinese companies issue their own ‘social credit’ scores under state-approved projects (Hatton, 2015). This case study might pose a larger challenge to research, as I expect information on the subject to not be plentiful, and challenging to dissect. The Chinese government expects to have started the program by 2020, so I will be making essentially an educated guess as to how this system will be constructed, making this case study different from the ground up from the other cases.

The Chinese government emphasizes the transparency advantages the social credit system will bring, as well as how rewarding good behavior and choices and punishing undesirable behavior could bring a safer and more harmonious society (Hatton, 2015). The different actors in the first part of this endeavor, including the Chinese government, online marketplace Alibaba and its financial wing Sesame Credit will be inspected through SCS, as well as the nonhuman actors, in this case the different ways in which data on citizens will be accumulated, stored, and analyzed. Indeed, this case might prove to be the most blatant function creep from our list, since the Chinese government makes no secret of its intent in increasing the scrutinizing of its citizens movements. This investigation takes place both off- and online, with over 20 million CCTV systems installed in public spaces (Langfitt, F. 2013), and digital surveillance in both computers and smartphones is prevalent (Fuhrman, 2016).

4.1.2 ANT into SCS

For this analysis, I will be following the translation by post-doc student Rogier Creemers, who released a translation of the ‘State Council Notice concerning Issuance of the Planning Outline for the Construction of a Social Credit System (2014-2020)’[6], and I will also be using information from news outlets, such as an article

[6] The translated ‘State Council Notice’ can be found here: https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/

in the Dutch Volkskrant[7]. This is the notice that many news outlets have used for outlining their coverage of this as well.

For this analysis, I will be researching the situation that China is aiming for in 2020. This means that the following analysis is based on the information from the council notice translated by Creemers (2014), news articles, and current situation in China. We will be analysing the translation of this hypothetical situation. This 'translation' will be following the explanation of translation in ANT from chapter 3. We can look at the Chinese government as the actant in the middle of this network. We may now keep calling it one actant, since it does not serve our purposes to zoom in further on this actant to see that it is of course comprised of many networks, which in turn include more networks comprising of many actants themselves. The actants (different departments) connected to the Chinese government will all be involved in the SCS, as the introductory sentence of the planning outline is as follows:

"All provincial, autonomous region and municipal People's Governments, all State Council ministries and commissions, all directly subordinate departments:

The "Planning Outline for the Construction of a Social Credit System (2014-2020)" is hereby issued to you, please implement it earnestly. (Creemers, 2014)"

No structure of government is left out, and the implementation would involve all governmental organizations, as well as all commercial and proprietary organizations that are condoned by the Chinese government (Creemers, 2014).

Problematization

The first step as described by Michael Callon (1984) in using ANT, is twofold. First, we will identify the basis of the situation, the 'problem' that needed solving that instigated the network formation. Second is the identification of the actants involved in that specific situation. The 'problem' in the case of the SCS is that the Chinese government seeks information on its citizens and their activities, to "establish a sincerity culture, (...) carrying forward traditional virtues and encouraging trust" (Creemers, 2014). This is a clear example of the 'social engineering' that has, according to some, kickstarted China's economic growth, as well as keeping the drive present in the public mind (Xia, 2003).

The government's 'want' is clear; it seeks to accumulate information on their citizens, whether it is to establish the sincerity culture as translated by Creemers, or in an effort to create a more controlled state: the result is the same. The first actants are connected by this want; internally, the government is activating its

[7] 'China kent elke burger score toe - ook voor internetgedrag' ('China to score every citizen - even for internet behavior'). De Volkskrant, 25-4-2015. Retrieved from: http://www.volkskrant.nl/buitenland/china-kent-elke-burger-score-toe-ook-voor-internetgedrag~a3980289/

different branches in order to achieve the collection of information. This happens through the policy document, which is also an actant in this network. Here, we are depunctionalizing the government. We may punctualize it again further on in this analysis, after the at first heterogeneous branches of the Chinese government that have not yet started working toward the same goal are informed and acting on their orders. The citizens are informed of the program, and as the direct objects of the program, together with businesses, they can also be identified as the actants involved. These businesses act in two ways within this network (Creemers, 2014). Firstly, they themselves are monitored. Secondly, they are expected to supply the SCS with the citizen information the system requests. There are also numerous non-human actants that are activated at this point. The infrastructure needed to move and store the large amounts of data on potentially all Chinese society participants is enormous (Persson, Vlaskamp & Obbema, 2015). All businesses from social media, online shops, financial institutions such as banks, to hospitals and doctors' offices are expected to be enrolled, and actively participating.

In the Communist Chinese State, the singular 'want' from the government activates many actants, showing a wave-like surge of force of power, first from the government's own divisions, to local hospitals and banks.

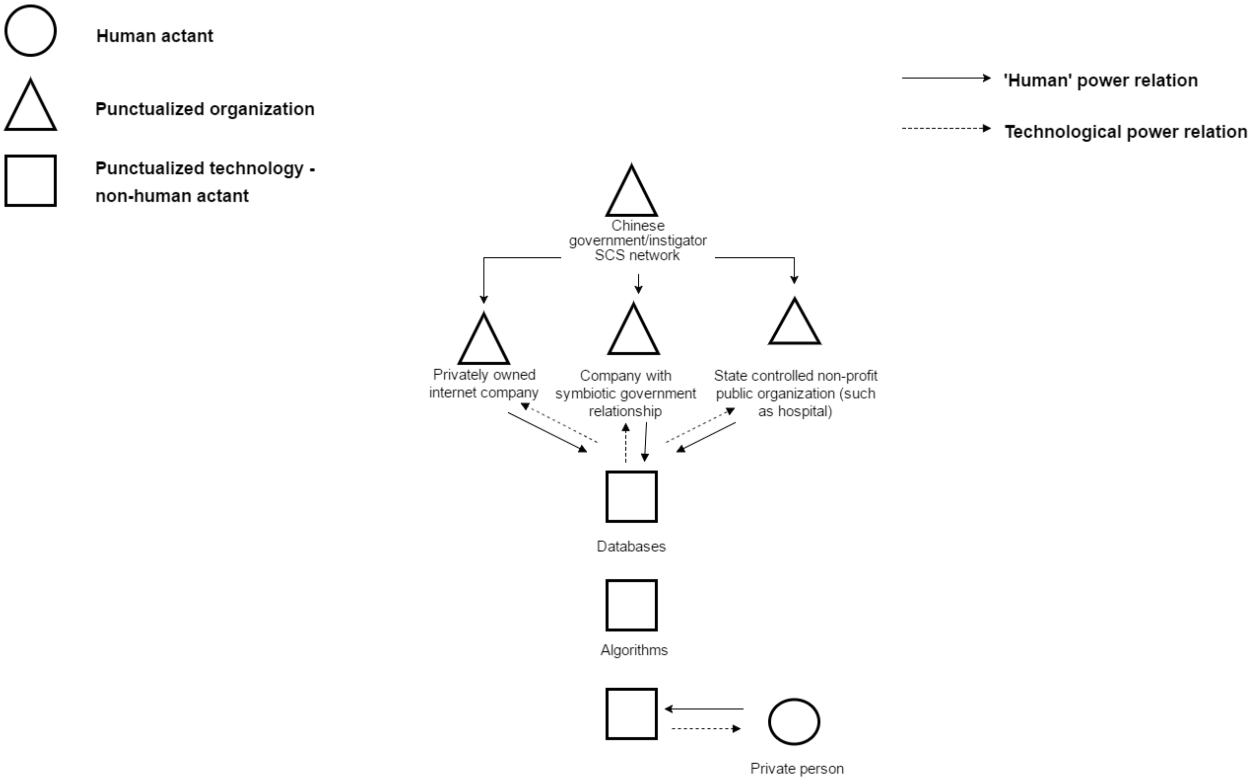
Interessement and Enrollment

In the 'interessement' phase, the network actually comes into being. The different actants are 'locked' into place, and the interplay between the actants evolves. In this situation, the Chinese government plans to endow individual citizens with positive scores when they themselves make 'good choices' in their lives. They may for example actively call out polluting businesses, or criminal activity in their environments (Persson, Vlaskamp & Obbema, 2015). This gives the individual power to influence their own credit scores; giving the individual more agency than if there was no such installment at all. Individual people would not be able to escape the SCS program, unless they would be willing to start living a hermit life; much social interaction takes place on social media, this is true for China as much as it is for Westerners (Chiu, Ip & Silverman, 2012). As explained, non-human actants like social media on computers and smartphones may create dependence by their users, in a similar sense to not being able to look away. It is as such a combination of technology and social pressure that works in the SCS's favor. According to McKinsey research, there were already 300 million Chinese people connected to social media in 2012, and this number has only expanded, with Weibo alone reaching 261 million monthly in the first quarter of this year (CIW, 2016).

In a combination of the 'interessement' and 'enrollment' phases, there is probably movement in the relations between government and private companies; Persson, Vlaskamp & Obbema (2015) theorize that these companies have different interests at heart, between pleasing the government's requests for information on their customers, and protecting these customers' privacy. Eventually, this will come down to the consumers' need to use the services offered by these companies, and their own potential 'want' to keep as much information about themselves, to themselves, as explained in the 'Privacy and surveillance' chapter.

The most present technological actants in the SCS network, are those employed by the Chinese state, and by the businesses to enact the SCS plan. This involves the technology needed to follow individuals as well as businesses, the technologies needed to create databases to store this information, and the algorithms that supply the SCS with the information needed, from the raw data input.

Below, I have inserted an illustration to detail an example of how these different actants could be present in this (simplified) flowchart:


Human actant
Punctualized organization
Punctualized technology - non-human actant
'Human' power relation
Technological power relation
Chinese government/instigator SCS network
Privately owned internet company
Company with symbiotic government relationship
State controlled non-profit public organization (such as hospital)
Databases
Algorithms
Private person

Since this network is such a complicated one, I have made the decision to only include the actants that cause the most translation to occur. The persuasion caused by the government (through the non-human actor which is the policy document) work to shape the other actants. The ‘human influence of power’ is controlled culturally, and politically. An intricate and complex process, a force leading other actants into action. This human power relation is opposed to the technological power relation.

Mobilization

Now that the network is stable, the actants start interacting. In one word, we can capture what is happening during the Social Credit System as surveillance. Top-down surveillance is the most common one in this situation: the government, seen as one actant, surveils all below, as seen in the flowchart above. The punctualized technology affords that to the organizations performing the surveillance. The Chinese government states in the Council Notice that it seeks harmony and transparency (Creemers, 2014), however, through the surveillance process that is organized through SCS, only social control is sure to be achieved. David Lyon tells us that through meticulous surveillance, social relations are further organized, leaving the Chinese government with more social power than before the implementation of SCS. This may leave the Chinese with a more ‘harmonious’ society, however, it leaves the power over this information in the hands of one actant, which is the beginning and might be the end of the network; the government. If it is successful in the introduction of the credit system, which will surely take years to implement, it will have gained an enormous centralized surveillance network, linking all Chinese people, and potentially calling them to order. The use of algorithms and computing power to make sense of the big data amounted from the system shows the empowering relationship between the non-human technological actants and the governmental bodies and other organizations employing them. The systems in which the algorithms are employed are likely given a set of data that is already categorized, which will allow for the system to use the algorithm to start looking for similar data, and then categorize it accordingly. The system has the agency to create useful information out of big data, which is caused by its relation to the algorithm in place. The use of systems like this, are an introduction of a panopticon type of surveillance; everything can be of effect to an individual’s credit score, since all information accessible to the system is utilized. This is likely to result in obedience and homogeneity: in the words of the State Council Notice: ‘harmony’ (Creemers, 2014). However far-reaching, it seems that Chinese nationals side with the surveillance, praising the safety it brings, and how extra surveillance measures heighten their ‘sense of satisfaction’ (Bakken, 2012). Creemers says that the way in which the SCS is portrayed in Western media is typical: “Pretty much anything China does makes people panicked” (...) “And many times we don’t recognise that we are doing similar things” (Hodson, 2015). He states that in the West, as opposed to China, it is often private companies carrying out the same level of scrutinization.

The SCS is a potential function creep, because the type of information accumulated by the government could be useful for other ends than SCS. It is not announced in the policy document, but it is likely, according to Creemers’ (2014) study, that the information gathered on citizens and businesses will be shared with law enforcement, creating an enormous database in which all citizens can be found, along with their personal details. Whether or not this use was not originally intended, the use of this information by law enforcement has not been communicated to the general public in the Chinese press (Persson, Vlaskamp &

Obbema, 2015). Since the 1990s, ‘weiwen,’ or ‘perpetuating social stability’, has been the government’s public mantra (Feng, 2003, p. 3), and the plan for the SCS seems to follow this creed very closely.

The SCS could backfire for the Chinese government: taking the paradox of control in mind, the increase of surveillance, and a function creep occurring in this surveillance would mean an accumulation of scrutinization for Chinese citizens. The problematic paradox would occur if the extra measures taken were to be regarded as the proverbial straw breaking the camel by the citizens being surveilled; their potential resistance to an expanded SCS would mean that the government’s objective of harmony would instead turn into an increase in government opposition.

4.1.3 Achmea

The next case is from The Netherlands. Dutch insurance provider Achmea has plans to start offering its clients a discount on their insurance fees if they are willing to opt in on a new program, first mentioned during an interview with an Achmea spokesperson in late 2015 (de Horde & Rolvink Couzy, 2015). The plan revolves around several devices that use different kinds of sensors and GPS that users will place in their cars and/or homes, which will then collect data on where the users go and when, and whether their homes are secure (Klompenhouwer, 2015). Achmea is talking to Google about working together on the Nest thermostat system, and is developing the the device for cars with GPS navigation company TomTom (Klompenhouwer, 2015).

Concerns about these undertakings have arisen, since Achmea might use the data against the user in finding ways to not turn out insurance money, as speculated by Bits of Freedom journalist Evelyn Austin (2015). Another possible issue is that the poorer the individual is, the likelier he or she is to choose the discount on their insurance bill, say organisations supporting citizens’ rights to privacy. Vincent Böhre, from the non-profit organization Privacy First, sees Achmea’s plan as privacy discrimination to the poor (Hofmans, T. 2015). Achmea themselves say that they pose their clients a ‘win-win’ scenario: Lower insurance rates and safer homes and cars for the clients may mean less insurance payouts for Achmea; an eye must be kept on the potential for a control paradox. I will investigate the power balances within this situation through ANT, and see the different roles of the actants involved.

As with the SCS, this situation revolves around a ‘proposed’ plan. The following actant network analysis will be based on the information relayed by Achmea spokespersons in both press releases, news articles, and similar sources.

4.1.4 ANT applied to Achmea’s smart home & smart car plans

The information that I will be using to assess Achmea’s proposed plan, is what the company itself has communicated to the public. I have access to publicly accessible press releases, and also will be using information provided through Achmea spokesperson interviews with (Dutch) news outlets.

Just as with the SCS case study, I will be following Callon's four moments of translation (1984, p. 59).

Problematization

We start off in the 'problematization' phase. What is the 'problem', and what are the actants involved?
The 'problem' is that Achmea would like access to their clients' information, so that the cost of claims can be reduced. They offer their clients, what they call, a win-win situation, in which Achmea is supplied with data on customer behavior, and the client receives, according to Achmea's director of Market Strategy Albert Spijkman, a safer living environment as well as a reduced insurance premium (de Horde & Rolvink Couzy, 2015). It is clear then which actant is the initiator of this network: the insurance company, Achmea, as a whole. When we depunctionalize it, we can identify further actants: Achmea's internal 'market and research' division, and its affiliated spokespersons, such as the previously mentioned Mr. Spijkman.This is how the company's plan was brought to the public ear; the director of market and research revealed the insurance company's long term intentions in an interview with Het Financieele Dagblad (the Dutch Financial Times).
In addition to Achmea's inner workings, when looking at what the plan entails, we can identify the subject of interest: the insurance policyholder. For this customer to enter the network and the potential function creep situation, he or she has to enroll in the program, which means that a policy document needs to be signed that both parties are then bound to. This document is another actant, a non-human one to be exact.
In the implementation, several non-human technological actants come into play. There is the little box in vehicles, which "will stimulate safer driving behavior" and the in-house technology, possibly internalized in Google's Nest system (Klompenhouwer, 2015). Nest is a 'house manager', including a carbon monoxide and smoke detectors, and thermostat in one (Google, 2016). Here, we can see the Internet of Things showing the possible implementations. Devices that are connected to each other, and the internet. If enabled through the program, the system will also collect the users' data, and send in to the insurance company. This data will be saved in a database, where algorithms most likely translate the raw data into usable data, potentially used by Achmea in any way they see fit.

Interessement and Enrollment

This is when the network is set into place, and the interaction between the actants begins. In this case, it means that first a client signs the agreement document with Achmea. This will most likely happen after persuasion on the part of Achmea, be it in the form of offering a discount, or convincing a home and car owner that it is the safest thing to do. The devices are now added to the network, installed in the home and car, and are connected to Achmea's database. Information is uploaded to this directory, and now Achmea can start using the data for their own analysis. All interaction detectable by the devices is monitored; by definition, this has become a surveillance operation. The data accumulated is attached to the users' personal information, meaning that it is not an anonymous database that they are adding to, in return for discounts.

The users most likely to choose this system, are people with lower incomes. They may not see the value in their data, and might need the financial relief offered by the program. If started, this program would be a prime example of what David Lyon (2003) meant by the ‘social sorting’ that happens when financial situations are intertwined with surveillance. This means that either ‘worth’ or ‘risk’, as explained by Lyon, (2003, p. 19), are assigned to specific people, which can have far-reaching consequences for their future. In this case, Achmea would most probably employ this type of surveillance to further specifically assign varying degrees of risk to ‘categories’ of people. This is of course something that insurance companies have been practicing for several years, most notably seen in the manner in which persons with a higher educational background enjoy lower vehicle insurance rates, due to the lower risk of damages statistically associated with these people (Gusner, 2013).

Mobilization

In this phase, the actants begin their interaction. The user agreement, and any matter in which Achmea would attempt to contact their clients in order to convince them to sign up for this program, would start with Achmea being less powerful than the client: the client may still not participate, and has the agency to resist. However, as soon as the agreement document is signed, this power shifts. The document has the inherent power of changing the relationship between client and company, leaving Achmea with their clients’ personal home- and vehicular information, while the client has no detailed explanation on what the company will do with that data, effectively leaving them powerless on that front. ‘What the company will do with that data’ is also where the function creep may appear. As a commenter on the Financieele Dagblad website theorizes, Achmea may well use the data ‘against’ the users in their investigation surrounding claims. For example, if a client has had an accident on their way to work, Achmea might claim that they were paying less attention because they were in a hurry ‘evidenced’ by their above average acceleration. Many people may be tempted by this program, especially when keeping the survey by EMC (2014) in mind, mentioned in chapter one: users of online services part with their personal information with ease, it may be assumed that they will part with their personal home information and vehicle data without reluctance, when presented with a financial incentive.

The Achmea plan is a ‘potential’ function creep, since the accumulation of the data on Achmea’s part could pose the company for interesting opportunities, that may not be initially communicated.

We will have to wait and see if the plan will actually be implemented, and whether Achmea will act on the opportunities that will rise from their access to personal data. These opportunities could be the example talked about in the previous paragraph, using the data ‘against’ their users, however, they could also be interested in sharing this data with third party companies, who in turn would very much be interested in the kinds of information Achmea would be gathering (Klompenhouwer, 2015). As made clear in chapter one, the paradox of control is not limited to disrupting initiatives on a governmental scale. It can also affect businesses, especially if they have emphasized consumer benefits publically: as mentioned, the paradox happens when the risks of enrolling in a certain situation are underestimated. In Achmea's case this could happen when, after reassuring the public that they themselves remain in control of their information, Achmea does proceed in additional practices, after being tempted by the (financial) benefits of using personal data. Indeed, for Achmea's plan to succeed, they will have to show their 'worthiness' of the information, as Taylor (p. 66) says, for these kinds of practices to succeed socially, they have to remain accountable. Regulation seems to be key here.

4.2 The 'Known' function creep cases

4.2.1 The UK sex offender register

In the case of the UK sex offender register, the group of people affected by its use is larger than one might initially believe it to be. In 1997, the UK government started registering designated offenders, requiring them to notify law enforcement every time personal information changes, such as their address or phone number (Thomas, p. 227). Terry Thomas, Professor of Criminal Justice Studies, wrote an exposé on how function creep perpetuated the introduction and further use of the register. The number of people on the list in 2006 was 30,000, all people who have a lifetime obligation to keep the UK authorities updated on wherever they go (Batty, 2006). This is however not the only use, in the years following 1997, the register has evolved with legislations adding more and more functions.
When the register was set up 1997, the UK Home Office stated the purpose of the register as follows:

- the register would help (the police) identify suspects once a crime had been committed;
- it could possibly help them to prevent such crimes (and)
- it might act as a deterrent to potential re-offenders (Home Office, 1996, para. 43).

The reason for taking the sex register as a 'known' case, is through the previously mentioned work of Terry Thomas, who has written on the sex register as a function creep in his 2008 paper, 'The sex offender 'register': A case study in function creep'. Thomas, professor of Criminal Justice studies at Leeds Met, adds that the Home Office has always stated that the register was not a form of punishment. It was put in place "to help protect the community from sex offenders" (Home Office/Scottish Executive 2001, p.11, in: Thomas, p.228).

Since the nineteen nineties, there have been numerous policies put in place to ‘strengthen’ the register, essentially increasing the function creep. An example is a change made in the early days of the register, that obligates people who have received a caution, as opposed to a sentence of any kind, to register. In the past, Thomas points out, a caution was a measure used by the police for people who had committed minor crimes, and who were unlikely to make similar mistakes again. This change brought with it the implication that cautions were serious enough to justify registration; that a caution meant that an offender would likely lapse into similar behavior (Thomas, 2008, p. 229). Other changes added over the years include registrants having to notify the police when going abroad for longer than eight days, and the police being given new powers to photograph and take fingerprints during offenders’ first registration visits. These changes, along with many more like them, have very large amounts of information associated with them, on a growing group of citizens, thereby potentially influencing their behavior and emotional state.

4.2.2 ANT into the UK sex offender register

I have more information available to me in the two ‘known’ function creep cases, for multiple reasons. The first, is that they have simply existed for longer. The second, is that they are both charged topics. There has been much to say about both in the media, and politicians have spent time debating them. In the case of the UK sex offender register, I will be basing my analysis on the findings of Terry Thomas and his peers, and the response the issue has provoked in online and written media.

In the previous analyses, I have been focusing on the ‘coming into existence’ of the two cases. For this case, I will be analyzing the period in which the function creep occurred, after the initial creation of the register.

Problematization

The register was proposed because of a singular emotion: fear. The advancements made from the start of the register onwards have always had grounds in the same emotion (Thomas, 2008). The basis for the start of this register falls in line with surveillance theory; as mentioned in chapter 1, the implementation of surveillance measures is made easier when the public is influenced emotionally. In addition, the importance of privacy for specific persons varies with their social status (Whitman, 2014). A person seen as a criminal, will have a smaller right to privacy in the eyes of the public than an ‘average citizen.

The sex offender register was initiated in 2008, following the USA’s lead in keeping a running record of those that had committed sexual offenses. Both local and national police forces in charge of the prosecution of sex offenders pressed the need for the existence of this register. The first actants in this situation can now be identified:

-The police (for now punctualized organization; depunctualized there are many different departments spread across regions and levels of authority)
-The sex offenders themselves (human actants)
-The UK Home Office, punctualized (the policy making branch in charge of immigration, security, and law and order)
-The register itself (a database within an existing criminal database; non-human actant)
The 'wants' in this case, which have given rise to the situation, come forth from the UK Home Office. According to some, the basis for the introduction of the register was a calculated electioneering move by politicians (Thomas, 2008). In any case, it was created as a means to improve child protection and community safety, says Thomas in his 2004 paper (p. 225) on the origins of the register.
Those were the initial wants for the creation of the register. The register was officially seen as a complete success in policy making, with Home Secretary John Reid saying that " (..) while these measures [the sex register] have greatly increased public protection from sex offenders, I believe we can still do much more (..)" (Home Office, 2007, p. 3). The register has been at the hands of changing wants over the years, meaning that the network of this situation has been in constant flux.

Interessement and Enrollment

In these moments, the network comes alive, and the actants are interacting. The actants are locked into place, driven by their 'wants'. In this case, I am focusing on the moment the policy is put into place, and how the interaction between the actants evolves from there. People that have broken the law and are then deemed sex offender due to the nature of their crime, are obligated to take part in registering with the police, and supplying them with personal details such as their home address. This interaction takes place because of the law; sex offenders are obligated to register, not doing so would have serious consequences. The agency of the (non-human actant) register (which it has gotten through the law-making of the Home Office) forces the sex offender to comply. Local police then process the information, which then is added digitally to the archive known as the sex offender register. This database containing the register allows police to access this information whenever they see fit (Thomas, 2008). Whenever a registered convict moves, he or she has to notify police, so that their entry in the database can be updated. This means that the interaction, and the effects of the register, are continuous. As long as the register remains, the registrant is under the influence of its agency.
Here, we may see Latour's theory in practice; instead of a gun and a man creating a gunman (see chapter 3), it is the database combined with a policy, and the subjects that are to be included in that database that make the sex offender register. By themselves, the combined actants are just that, actants. However, connecting these actants creates interaction that leads to larger amounts of agency for the created entity.

Mobilization

In the mobility phase, the actual interaction between actants begins; the network is played out, and this is the moment in which a network proves itself viable. The sex offender register is a network that has transformed several times since 1997. These changes occur when the wants of one of the actants change, or when the power relations are made unequal by external changes. Often it is a combination of both. In this case, changes were made to the register by policy makers responding to some particular crimes being committed. By doing this, they were the ones who protected children and stood for safety in their communities (Thomas, 2004, p. 227). The first (and originally, only) function of the register was to make sex offenders register with local police departments, so that the police would know where they were at all times. One additional function was already added while the bill was in the last parliamentary stages; police cautions were added in, in addition to conviction, which previously was the sole proposed precursor to registration, says Thomas (2008, p. 229). This might seem like a small change to some, but as explained in the introduction of this case on **PAGE,** a caution means that a person is not convicted of a crime, however, after this change, they have to register along with those convicted of a sex crime. As Thomas points out (2008, p. 229), this carries the assumption that someone who has been cautioned, will likely do whatever they were cautioned for, again. In addition to this early change, seven other major changes were made. These range from increasing the sentence for non-compliance to a maximum of five years instead of six months; having to inform authorities with one's whereabouts within eight days instead of the previous fourteen days; and allowing the police to search a sex offender's residence with a warrant without 'regular' probable cause. In addition, the range of crimes an offender has to commit to be labeled 'sex offender' was widened several times, leading to the following crimes being marked as prerequisites for being included in the register:

"(...)
burglary with intent to steal,
inflict grievous bodily harm or do unlawful damage;
child abduction;
harassment;
and sending prohibited articles by post" (Thomas, 2008, p. 234).

Even though these crimes are not inherently sexual in nature, the Home Office explained that:
"(...) the offences may not seem inherently sexual, but could have had a sexual motive. These changes are necessary to strengthen the monitoring and management of sex offenders". (Home Office, 2006)
The (punctualized) actant with the most driving force, and agency, is clearly the Home Office. The register itself gains more agency as more changes occur, and the network remains intact, albeit in a changed form. Each time these changes are implemented, the 'rules' of how the network is translated, changes. More actants are incorporated, for example, the human actants that would previously not be included in the register for their crime, but now have to comply.

These above changes are what makes the register worrisome, according to Thomas (2008). Few people would say ‘no’ to a measure that would make the lives of children safer, keeping in line with Whitman’s (2014) theory of how public perception can strongly influence a person’s right to privacy. However, there has not been evidence of the register achieving this (Plotnikoff & Woolfson, p.50). Instead, the increasing function creep has made the register turn more into a punishment than a preventative measure, while keeping the power relation between law enforcement and registrant in place.

The function creep that has occurred here is clear: over several years, the UK Home Office has ‘strengthened’ - built on top of- the existing register. These changes were not presented in the original plan for this policy, and as such qualify as function creep. When looking at how this particular function creep came to be, it seems to diverge from the other cases. It was not sprung from access to technology, and the promise of this technology to make the world a better place. The database for this register might well be kept on paper, which would be terribly inefficient, but possible. However, the function creep in this situation sprung from fear; fear that needed addressing. A multitude of changes over two decades followed, impacting the lives of many. This function creep has led to a question that needs considering; has this register, after being subject to many changes since 1997, transformed from being a policy put into place to protect the safety of children, to something that resembles life-long punishment? This punishment takes the shape of a construction resembling the panopticon discussed in chapter one: the people affected by the register are continuously reminded that they are registered through their obligation to keep authorities updated and by having the knowledge that they can be watched at any time if these same authorities were interested. This is also where my theory for the control paradox partially stems from: the UK Home Office initiated the plan for the sex offender register to protect and provide security for UK citizens. After the function creep has taken place, the register has paradoxically become a burden to a still increasing group of citizens, many who are indeed sexual offenders, however, also including others who would not have been included in the first version of the register, due to the non-sexual nature of their offence, or even because they were merely cautioned, and not convicted of an offence.

4.2.3 The use of biometric data in Dutch passports

From 2009 onwards, the Dutch government has been obligating all citizens who apply for a passport to provide their fingerprints and to be subjected to a facescan, which are then added digitally to the passport, on a chip. The purpose of this plan was to prevent identity theft and related fraudulent activities, through the incorporation of this biometric data (Heck & Kas 2009). However, even though the plan was presented as such, there were other functions claimed later on in the ‘passport law’ that soon followed: Dutch law enforcement would be free to use the data for their purposes, which is a different use of the data that citizens were entrusting the government with (Huissen, 2010). The database filled with biometric data proved too useful not to use in other contexts, apparently. In 2014, regulations were toned down regarding the national Dutch identity card, which, in addition to a driver's license, is one of three legal documents that a Dutch person can use to identify themselves with in the Netherlands. When a person does not wish to provide their fingerprints to receive this identity card (essentially a passport, however, it is for national and limited EU use), they do not have to do so anymore. Civil rights organizations had been fighting the accumulation of data on RFID chips in means of identification, since they believe the Dutch government to be unprepared in terms of the security of keeping this information in a central database. The possible dangers of this plan would only be enlarged if other functions or uses were added, say spokespersons for these organizations (Huissen, 2010). Law enforcement officials are able to access the database for investigative purposes, to identify people; this is a function of this database, that was not discussed at the introduction, and was not the said reason for the erection of the database. Speculations have arisen if the database was merely a privacy breaching measure in the disguise of anti-fraud regulations (Huissen, 2010). In the best case scenario, the biometric database was started with good intentions following security concerns, and later accessed by law enforcement and the public defender's office.

4.2.4 ANT into biometric data use for Dutch passports

Problematization

The 'problem' that the Dutch government, the main actant, was addressing was the fraudulent altering and the identity theft using passports. These passports, which are to be subjected to security measures, are one of the major non-human actants. In this situation, it is interesting to address that there is an apparent discrepancy between the problem that is being solved, and the 'want' of the same government. I am now punctualizing this government, however, it seems likely that to attribute the problem and the want, we will have to depunctualize this structure slightly. For it seems that the solution to the 'problem' in this situation answers the 'want' of another part of the government; one that is discovered when Dutch law enforcement is depunctualized. There are two departments important here, that are not thoroughly interlinked, and work independently; there is the 'Koninklijke Marechaussee', the royal military police, and there is the Dutch national police (Rijksoverheid, 2012). The military police is responsible for the prevention of identity fraud, and the national police has no part in advising on the policy making on this subject. After this depunctualization, we will need to keep the government depunctualized partially: we have both the national police, and the military police as actants. The problem is grounded with the military police, as they are responsible for identity theft- and fraud prevention, while there is a 'want' from the national police for the data collected through the solution to the 'problem'.

Other actants in this situation include the technological non-human actants: the RFID chips, which, when depunctualized, hold data such as fingerprints and face scans[8].

To summarize, the active actants in his network are:

-The military police

-The national police

-The law proposal

Followed by, after the implementation of the bill:

-Citizens applying for passports

-Citizens applying for identity cards

-Passports & identity cards

Technological actants after depunctualizing these:

-RFID chips (on which to store data: -Fingerprints and -Face scans)

Interessement & Enrollment

As the network comes into existence, the agencies of the two law enforcement departments start intertwining; this is shown in the way that law enforcement access was drafted into the final law proposal, before it was implemented, but after the plans of the military police had gone public. This network has gone through two stages, and in the second stage, where the law was implemented, citizens and their documents are included in the network. The agency of the military police has launched this network, and continues to support it, through the town hall desks where citizens request and receive their personal documentation. Without providing their fingerprints, and in the case of passports facescans, they will not receive said documentation. This puts them at the weaker end of a power relation between them and the responsible departments. For traveling citizens, it is not an option to forego the renewal of a passport. In this sense, they are forced to cooperate, and leave their personal data, which now includes fingerprints and face scans, in addition to the information the government database has previously amassed on them.

In a sense, this case is similar to the UK sex offender case; here, there is also a power relation between government and citizen that is unequal, and involves an information database that is accessible by law enforcement. The obvious difference is the criminal status of the citizens involved; however, it is imaginable

[8] NOTE: Nowadays (2016), lawmakers have done away with the face scans, meaning from 2014 onwards, citizens renewing or requesting a passport will 'only' have to supply their fingerprints.

that in both situations a citizen could feel just as pressured to give up this sensitive personal information to add to these databases. A citizen might just *have* to travel, and they *must* have proper documentation, just as a sex offender (or a burglar with just a caution) *has* to update the government on their whereabouts whenever their situation changes.

Just like with the UK register, it seems that the citizen who gives up their information as a means to an end (to obtain a passport for traveling), does not have any control of the data they are supplying to these databases. The agency of the database is far reaching; bestowed upon it through the information it holds. The information is very useful to the national police, since they may be able to link people to fingerprints and solve crimes that way. This means that the system may have the effects the law enforcement departments are counting on: decreased fraud in passport forging, and identity theft (Rijksoverheid, 2011).

Mobilization

The network is in full movement in the mobilization phase. People who renew their passports and identity cards, or request new ones, are confronted with the regulation. They will feel forced to provide their fingerprints and face scan, for else they would not be able to travel. This information is then added to this database, which has a large amount of potential, and therefor agency, when seen in relation to the national police. However, it could be theorized that the people with the least money, are also less likely to travel, and a passport would not be very useful if one never leaves the country. Here we see David Lyon's social sorting (2010) at work again; potentially, an entire group of citizens with the lowest incomes are not included in this 'program', and do not provide the database with their fingerprints. This would mean that this database is not a reflection of the current Dutch society, but only of that part of citizens that will travel outside of the Dutch borders, and as such, the database may have limited use for the national police.

The potential of future cross correlation between databases (be they law enforcement or perhaps medical) could imply for far reaching consequences for citizens and law enforcement departments involved. This cross correlation could mean categorization as mentioned in the 'Privacy and Surveillance' chapter, which would allow for a systematic search for possible safety hazards, as well as pose a challenge to citizens looking to retain privacy; impossible, especially when the government's agency is aided through posing the surveillance measures as prerequisites for, for example, needed personal documentation. In addition, the weight of the measures taken to prevent identity theft for a very small group of citizens can be seen as not to weigh up to the surveillance occurring to prevent this. As Harris et al. (1995) explains, different levels of surveillance fit different levels of security threats.

The implementation of the Dutch passports fitted with RFID chips is a clear cut case of function creep: a database built for one purpose, is used differently than 'advertised', which has consequences for all involved. In addition, citizens are affected by the system in varying degrees: people who travel outside of the Netherlands would be included in the database, whereas people who do not cross the border, will not be.

This could have implications for a specific kind of categorization, in which the wealthier middle-upper class would be included, whereas people of fewer means would see no need for a passport.

Similar to the UK sex offender register, the Dutch passports fitted with biometric data have paradoxically become an almost nation-wide burden, even though the initial plans were to protect a limited number of citizens from falling victim to identity fraud. The added functions, and the potential to law enforcement to search the database, have made citizens doubt the government, and initiated feelings of unsafety (Huissen, 2010), in contrast to the intended goal.

In conclusion, whether the negative outcomes (primarily found in the personal privacy of the citizen) outweigh the crime reducing effects remains to be determined.

5. Conclusion and discussion

I will first discuss the results of my research in the context of the two statements made in the introduction. To reiterate, they are the following:

- We can recognize future function creep cases by examining ‘known’ and ‘potential’ cases by following the power relationships occurring in the actor networks that make up these function creep situations;
- Function creep is a natural occurrence in our technology driven consumer culture, and has ambiguous consequences.

Firstly, can we now identify future function creep cases by going by my findings?

By reviewing four separate cases, from three different countries, I believe I have seen the variety in which function creep can occur in surveillance situations.

I have discovered that function creep occurs when ‘temptation’ exists. This comes in the form of available technology, able to record and keep information. Organizations such as governments and for-profit companies both give in to this. This could happen with the data available to Achmea in the future, and has happened with the biometric passport database. As explained in chapter one, often in the case of profit driven online-based companies, giving in to this temptation will not necessarily lead to a decreased client base or use of product (Davidson, 2014). In addition, I have found that function creep is likely to occur in instances where the surveillance measures chosen do not weigh up to the danger the measures are used to prevent (such as in the case of the Dutch biometric database, and the UK sex offender register). This is where the writings Harris et al. (1995) come into view; indeed, the balance between citizen and consumer privacy is disrupted as soon as function creep takes place. Moreover, the surveillance conducted can be seen as extreme measures to reach a particular goal (such as in the case of the Social Credit System as part of weiwen policies, to promote a harmonious Chinese society). I have also found that function creep in surveillance situations is perceived differently when practiced by for-profit companies as opposed to government surveillance. It seems that companies are expected to be practicing data mining and other surveillance tactics, which people are willing to forgive in exchange for the use of their services - and perhaps an insurance discount in the future. However, governmental surveillance and the function creeps occurring in these policies have met with criticism from citizens' rights movements and mainstream media, reflecting that function creep in surveillance is not welcomed in either case.

The second statement, as mentioned in the introduction, is on how function creep might be inherent to our current culture, with the access to technology we now use and need.

The need for the use of technology that is at risk for function creep is clear; we use Gmail and other services like it every day, and do not seem to mind too much that the companies providing these services use our data for their own purposes (Davidson, 2015).

The increase in transparency in policy mentioned above might be the solution for companies seeking to incorporate data use in new business ventures, such as Achmea. When people are informed of the exact use of the data, they can decide for themselves whether they find Achmea 'worthy' of their data, as Taylor (p.66) suggested. Transparency followed by accountability is the only way in which the use of personal data for profits can be socially and publically accepted.

In light of this research, I believe that the progression inherent to the function creeps discussed were natural progressions, and indeed stem from the temptation posed by the opportunities acted upon. I also believe that function creeps would not be function creeps if there had been a correct manner in acting on those temptations. Communication with the public is key, and if companies and governments continue to progress their products and policies quietly and with great expense to the privacy of those affected, a public debate cannot be held. To conclude, if positive changes occur out of function creep, such as increasing public safety or adding to the user experience of a product, it is no longer a function creep, instead, it becomes the natural progression of a product or policy.

Through my analyses, I have found that function creep is likely to occur when a service or policy is initiated that from the very beginning has access to citizen or consumer data; this was true for all of the cases reviewed. If this data can be used for commercial purposes, or for security measures, function creep is essentially bound to occur.

Most significantly, function creep occurs in situations where the balance of power is off. It develops in instances where the surveillers are the ones holding the reigns, instead of the people supplying their personal data. Through my analyses, I followed the power relations for this reason; function creep occurs because surveillers are tempted, and because they believe they can achieve their goal without negative repercussions to themselves.

If the goal is to limit the occurrences of function creep, transparency would be the only way to achieve this. This is shown in the way in which programs that were founded on good intentions spiral out of control of the organization watching over it. For example, the way in which both the biometric passport measure and the UK sex offender register were created out of a need to solve a particular problem. These problems were identity fraud, and the felt need to keep track of sex offenders. Over time, additional uses were created for these measures. The transparency needed translates directly to a much used saying in privacy debates - Who watches the watchers?

My main argument

What I have found, can be boiled down to the essence of the paradox of control. When one feels in control of a situation, the further it can slip out of control due to the increased risks taken, as explained by Brandimarte, Acquisti & Loewenstein. I have argued that the underlying feeling of control that can be present in individuals that then leads to them taking more risks, is also an occurrence in policy making and business advances. Two prime examples of this occurring are the ‘known’ function creep cases I have analyzed; both the sex offender register and the biometric passport spiraled away from the intended purpose, through different factors. In the cases of Achmea and the Chinese SCS, the potential control paradox could indeed also occur when they would try to delve deeper into citizen and consumer data. In the case of Achmea, they have stated that their main objective is safety, and what is a win-win situation for both the person insured as well as the company. However, the potential increase in data surveillance could lead to the person feeling less safe, and would most definitely change the situation to Achmea’s benefit. In essence, most of the programs to accumulate and use data for a singular well-intended purpose would be brought to imbalance the moment other purposes would be brought to the table.

I argue that this paradox of control is the agency of the ICTs used in surveillance situations that increase the risk-taking in surveillance situations, resulting in a function creep in these situations.

Advice for further research

Further research into function creep occurring in surveillance situations would have to take place on a larger scale, taking into account more cases, to further examine the occurrence of the control paradox. This larger scale is necessary, for the use of databases and the accumulation of user data will only keep growing in the coming years. The 'Internet of Things' is just around the corner, presenting companies and regimes alike with many new ways in which they may create reach their goals, undoubtedly presenting these same organizations with the paradox of control.

Bibliography

Austin, E. (2015). Achmea: vrije keuze of crowdforcing? *Bits of Freedom.* Retrieved from https://www.bof.nl/2015/10/01/achmea-vrije-keuze-of-crowdforcing/

Bakken, B. (2013). Keep smiling! - You're being watched. *The China Story.* Retrieved from https://www.thechinastory.org/2012/12/keep-smiling-you-are-being-watched/

Batty, D. (2006). Q&A: the sex offenders regiser. *The Guardian*. Retrieved from: https://www.theguardian.com/society/2006/jan/18/childrensservices.politics1

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: privacy and the control paradox. Social Psychological and Personality Science,4(3), 340-347.

Cain Miller, C. (2013). Google Accused of Wiretapping in Gmail scans. *The New York Times.* Retrieved from: http://www.nytimes.com/2013/10/02/technology/google-accused-of-wiretapping-in-gmail-scans.html

Callon, M. (1984). Some elements of a sociology of translation: domestication of the scallops and the fishermen of St Brieuc Bay. *The Sociological Review*,*32*(S1), 196-233.

Chishti, M. & Bergaron, C. (2011). Post-9/11 Policies Dramatically Alter the U.S. Immigration Landscape. *Migration Policy Institute.* Retrieved from: http://www.migrationpolicy.org/article/post-911-policies-dramatically-alter-us-immigration-landscape

Chiu, C., Ip, C. & Silverman, A. (2012). Understanding social media in China. *McKinsey Quarterly*. Retrieved from: http://www.mckinsey.com/business-functions/marketing-and-sales/our-insights/understanding-social-media-in-china

CIW. (2016). 85% Weibo monthly active users from mobile in Q1 2016. *China Internet Watch.* Retrieved from: http://www.chinainternetwatch.com/17509/weibo-q1-2016/

Creemers, R. Planning outline for the construction of a social credit system. Translation of Chinese original. Retrieved from https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/

Davidson, J. (2014). You Say You'd Give Up Online Convenience for Privacy — But You're Lying. *Time Magazine: Money*. Retrieved from: http://time.com/money/2902134/you-say-youd-give-up-online-convenience-for-privacy-but-youre-lying/

De Horde, C. & Rolvink Couzy, F. (2015). Achmea geeft premiekorting aan klant die data levert. *Het Financieele Dagblad.* Retrieved from: http://fd.nl/economie-politiek/1120827/achmea-geeft-premiekorting-aan-klant-die-data-levert

Dougherty, C. (2016). Alphabet, Google's Parent Company, Grows Briskly to Close In on Apple. *The New York Times.* Retrieved from: http://www.nytimes.com/2016/02/02/technology/alphabet-earnings-google.html

EMC Corporation. (2014). EMC Privacy Index. Retrieved from: http://www.emc.com/campaign/privacy-index/global.htm

Federal Trade Commission. (2012). Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser. Retrieved from: https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented

Feng, C. (2013). The dilemma of stability preservation in China. *Journal of Current Chinese Affairs*, 42, 2, 3–19.

Foucault, M. (1977). *Discipline and punish: The birth of the prison*. Vintage.

Fuhrman, P. (2016). Government cyber surveillance is the norm in China - and it's popular. *The Washington Post.* Retrieved from: https://www.washingtonpost.com/opinions/cyber-surveillance-is-a-way-of-life-in-china/2016/01/29/e4e856dc-c476-11e5-a4aa-f25866ba0dc6_story.html

Gartner (2013). Gartner says the Internet of Things installed base will grow to 26 billion units by 2020. *Gartner Newsroom*. Retrieved from: http://www.gartner.com/newsroom/id/2636073

Google, 2016. Meet the 3rd gen Nest learning thermostat. *Video on Nest.com.* Retrieved from: https://nest.com/#meet-the-nest-learning-thermostat

Greimas, A. et al.(1982). *Semiotics and language: An analytical dictionary* (p. 278). Bloomington: Indiana University Press.

Gusner, P. (2013). Higher education equals lower car insurance. *Nasdaq.* Retrieved from: http://www.nasdaq.com/article/higher-education-equals-lower-car-insurance-cm248522

Harris, D., O'Boyle, M., Bates, E., & Buckley, C. (2014). *Law of the European convention on human rights*. Oxford University Press, USA.

Hatton, C. (2015). China's 'social credit': Beijing sets up huge system. *BBC News.* Retrieved from: http://www.bbc.co.uk/news/world-asia-china-34592186

Heck, W. & Kas, A. (2009). Een paspoort? Dan wil ik graag ook uw vingerafdruk. *NRC.nl archief.* Retrieved from: http://vorige.nrc.nl/achtergrond/article2362556.ece/Een_paspoort_Dan_wil_ik_ook_uw_vingerafdruk

Hodson, H. (2015). Inside China's plan to give every citizen a character score. *New Scientist*. Retrieved from: https://www.newscientist.com/article/dn28314-inside-chinas-plan-to-give-every-citizen-a-character-score/

Hofmans, T. (2015). Privacy-organisaties fel tegen omstreden plannen Achmea. *PCMWeb.* Retrieved from: http://www.pcmweb.nl/nieuws/privacy-organisaties-fel-tegen-omstreden-plannen-achmea.html

Home Office (2006). 'Sex offender register to expand to include more offences', Home Office Press Release, 18 December.

Home Office. (2007). Review of the Protection of Children from Sex Offenders. Retrieved from [PDF]: http://webarchive.nationalarchives.gov.uk/20100413151441/http:/www.homeoffice.gov.uk/documents/CSOR/

Horwitz, S. & Markon, J. (2014). Racial profiling will still be allowed at airports, along border despite new policy. *The Washington Post.* Retrieved from: https://www.washingtonpost.com/politics/racial-profiling-will-still-be-allowed-at-airports-along-border-despite-new-policy/2014/12/05/a4cda2f2-7ccc-11e4-84d4-7c896b90abdc_story.html

Howell, K. (2014). Racial profiling at border stops, airports allowed under new federal guidelines. *The Washington Times.* Retrieved from: http://www.washingtontimes.com/news/2014/dec/6/racial-profiling-border-stops-airports-allowed-und/

Huissen, R. (2010). De rekbare doelen van de vingerafdrukkendatabase. *Platform bescherming burgerrechten.* Retrieved from: https://platformburgerrechten.nl/2010/09/18/de-rekbare-doelen-van-de-vingerafdrukkendatabase/

Klompenhouwer, L. (2015). Achmea wil lagere premie bieden als klanten privégegevens delen. *NRC.* Retrieved from: http://www.nrc.nl/nieuws/2015/10/01/achmea-wil-lagere-premie-bieden-als-klanten-privegegevens-delen

Langfitt, F. (2013). In China, beware: a camera may be watching you. *NPR.* Retrieved from: http://www.npr.org/2013/01/29/170469038/in-china-beware-a-camera-may-be-watching-you

Latour, B. (1999). *Pandora's hope: essays on the reality of science studies*. Harvard University Press.

Law, J. (1992). Notes on the theory of the actor-network: Ordering, strategy, and heterogeneity. *Systems practice*, *5*(4), 379-393.

Law, J. (2009). Actor network theory and material semiotics. *The new Blackwell companion to social theory*, *3*, 141-158.

Lohr, S. (2014). The privacy paradox, a challenge for business. *The New York Times.* Retrieved from: http://bits.blogs.nytimes.com/2014/06/12/the-privacy-paradox-a-challenge-for-business/?_php=true&_type=blogs&_r=1

Lynch, J. (2014). FBI Plans to Have 52 Million Photos in its NGI Face Recognition Database by Next Year. *Electronic Frontier Federation.*

Lyon, D. (2003). *Surveillance as social sorting: Privacy, risk, and digital discrimination*. Psychology Press.

Lyon, D. (2010). Surveillance, power and everyday life. In *Emerging Digital Spaces in Contemporary Society* (pp. 107-120). Palgrave Macmillan UK.

Mason, M. K. (2012). Foucault and his Panopticon. http://www.moyak.com/papers/michel-foucault-power.html *Retrieved May*, *17*, 2015.

Maurits, M. (2013). Nee, je hebt wél iets te verbergen. De Correspondent. Retrieved from: https://decorrespondent.nl/209/Nee-je-hebt-wel-iets-te-verbergen/6428004-ab2d5fc2

Moss, J. (2014). The internet of things: unlocking the marketing potential. *The Guardian.* Retrieved from http://www.theguardian.com/media-network/media-network-blog/2014/jun/20/internet-things-marketing-potential-data

NHTSA (National Highway Traffic Safety Administration) (2001). Event data recorders: summary of findings. Retrieved from (PDF): https://www.google.nl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjfpIem86TNAhXBOBQKHfKeAOkQFggeMAA&url=http%3A%2F%2Fwww.nhtsa.gov%2FDOT%2FNHTSA%2FNRD%2FArticles%2FEDR%2FPDF%2FResearch%2FNHTSA_EDRTruckBusFINAL.pdf&usg=AFQjCNFvnlD6-czzjtpPj4punuc2pHwRzg&sig2=A_7MyEEdtJK9DHyVm7-YEA

Nicas, J. (2015). How airlines mine personal data in-flight. *Wall Street Journal.* Retrieved from: http://www.wsj.com/articles/SB10001424052702304384104579139923818792360

Persson, M. Vlaskamp, M. & Obbema, F. (2015). China kent elke burger score toe - ook voor internetgedrag. *De Volkskrant.* Retrieved from: http://www.volkskrant.nl/buitenland/china-kent-elke-burger-score-toe-ook-voor-internetgedrag~a3980289/

Plotnikoff, J. and Woolfson, R. (2000) Where are they Now? An Evaluation of Sex Offender Registration in England and Wales (Police Research Series Paper 126), London: Home Office.

Rijksoverheid. (2011). Kabinet versterkt aanpak identiteitsfraude. *News article, Rijksoverheid.* Retrieved from: https://www.rijksoverheid.nl/actueel/nieuws/2011/09/16/kabinet-versterkt-aanpak-identiteitsfraude

Rijksoverheid. (2012). Inrichtingsplan Nationale Politie. *Kamerstuk, Rijksoverheid.* Retrieved from: https://www.rijksoverheid.nl/documenten/kamerstukken/2012/12/07/inrichtingsplan-nationale-politie

Ritzer, G. (2004). Actor Network Theory. *Encyclopedia of Social Theory*, *2*, 1.

Saetnan, A. R., Lomell, H. M., & Wiecek, C. (2002). Controlling CCTV in public spaces: Is privacy the (only) issue? Reflections on Norwegian and Danish observations. *Surveillance & Society*, *2*(2/3).

Simomite, T. (2016). Tesla knows when a crash is your fault, and other carmakers soon will, too. *MIT Technology Review.* Retrieved from:

https://www.technologyreview.com/s/601657/tesla-knows-when-a-crash-is-your-fault-and-other-carmakers-soon-will-too/#/set/id/601644/

Streitfeld, D. (2013). Google Concedes That Drive-By Prying Violated Privacy. *The New York Times*. Retrieved from: http://www.nytimes.com/2013/03/13/technology/google-pays-fine-over-street-view-privacy-breach.html

Taylor, N. (2002). State Surveillance and the Right to Privacy. *Surveillance & Society*, *1*(1), 66-85.

Thomas, T. (2004). Sex offender registers and monitoring. *Research Highlights in Social Work*. 225-248.

Thomas, T. (2008). The sex offender 'register': A case study in function creep.*The Howard journal of criminal justice*, *47*(3), 227-237.

Whitman, J. Q. (2004). The two western cultures of privacy: dignity versus liberty. *Yale Law Journal*, 1151-1221.

Wood, D. M. (2007). Beyond the Panopticon? Foucault and surveillance studies. *Space, knowledge and power: Foucault and geography*, 245-263.

Xiao, M. (2003). Social engineers for China's transformation and the 'visible hand'. *The New York Times.* Retrieved from: http://www.nytimes.com/ref/college/coll-china-politics-001.html

Zenger, R. (2012). Function creep is dagelijkse realiteit. *Bits of Freedom.* Retrieved from: https://www.bof.nl/2012/11/13/function-creep-is-dagelijkse-realiteit/