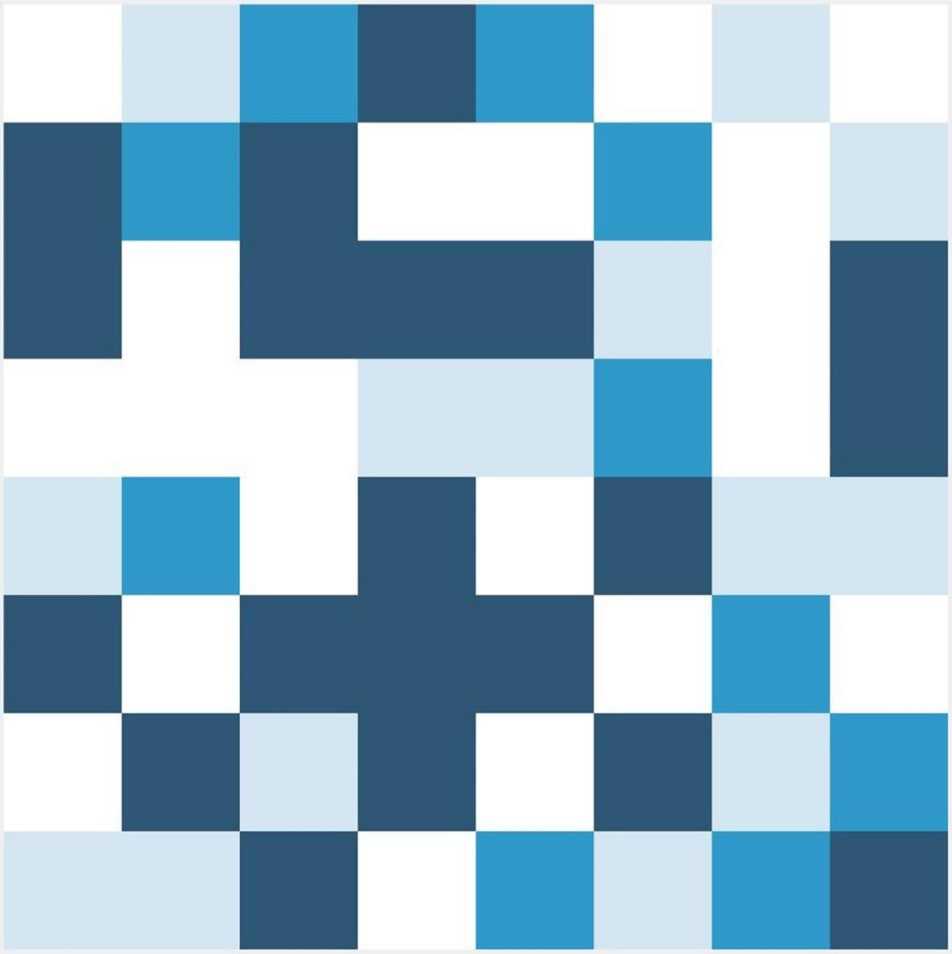
When Icarus Flew too High:

Moral Mediation in Mobile Instant Messaging Apps



This image is a visualization of the encryption key for this secret chat with **Gerwin**

If this image looks the same on **Gerwin's** phone your chat is 200% secure

Master Thesis New Media and Digital Culture
By: Gerwin van Schie (3807495)
Supervisor: Dr. Mirko Tobias Schäfer
Second Reader: Dr. Stefan Werning

I would like to thank my father for his unconditional support and trust. Without him it would have been impossible to finish my masters successfully.

Ik zou graag mijn vader bedanken voor zijn onvoorwaardelijke steun en vertrouwen. Zonder hem zou het succesvol afronden van mijn master onmogelijk zijn geweest.

Contents

List of images

1. Introduction

In his book *Op de vleugels van Icarus* (On the wings of Icarus), Peter Paul Verbeek (2014) uses the myth of Daedalus and Icarus as a metaphor to explain how society should treat new and developing technologies. In this story, Daedalus created wings for his son Icarus and himself to escape from the labyrinth they were trapped in. For the wings he used wax to attach feathers to a wooden frame which made the construction vulnerable. In order to arrive on safe ground they could not fly too high, because the sun would melt the wax and they would fall in the sea. If they would fly too low, the feathers would absorb water, making them too heavy to fly. Verbeek compares western society with all its technologies with Icarus and his wings. By analyzing how morality is mediated by the technology both designers and society could anticipate the possible effects and actively engage with them. Instead of asking ourselves if certain new technologies and their effects are desirable, rather we should think of ways in which we can actively guide these technologies. With this approach we as a society could, according to Verbeek, find the ground between being overconfident and coming too close to the melting rays of the sun and acting cowardly and drowning in the sea.

The field of big data and surveillance technologies is a much debated area in which society is trying to guide its technological developments. In politics this debate usually concerns the balance between privacy and security. After whistle blower Edward Snowden showed the world the practices of the National Security Agency (NSA) of the United States in early June 2013, we became aware of the fact that they, together with their United Kingdom, Canadian, Australian and New Zealand counterparts, collect and analyze almost all electronic communication it can gather. It even has an interface called “X-KEYSCORE” that taps directly in the databases of several big communication companies such as, amongst others, Apple, Google, Yahoo!, Facebook and Microsoft (Greenwald 2014). After Snowden’s revelations the spotlight turned to the privacy provided by online communication services. Most popular services proved to be insecure and were subjected to surveillance by the NSA. This resulted in the popularization of alternative services such as the TOR-browser, a secure internet browser, and Telegram, a secure version of WhatsApp (Dredge 2014). These alternative versions can be seen as the natural resistance against unwanted forces in a capitalist democracy. Society itself is guiding technologies in a preferred direction. Just as airbags and

seatbelts have become standard in car safety, encryption is becoming a standard in communication privacy.

Before only a few people were using encrypted and secure services, but now even popular and mainstream communication companies have to show they are thinking about the privacy of their users (Dredge 2014). WhatsApp, currently the most used messaging service, partnered up with the encryption company Open Whisper Systems in December 2014 and started to use so called End-to-End encryption in January 2015 (Greenberg 2014; Open Whisper Systems 2014). The thought that soon it would be impossible to access the messages of the worlds most used messaging service was worrying the political leaders of the United States and the United Kingdom. Barack Obama stated that encryption was allowed but he pleaded for the creation of a "backdoor" for the government (Oremus 2015). David Cameron, the Prime Minister of the UK, went even further and said, in several instances, he would take action if Britain's intelligence services were not able to get access to the sensitive information that might be shared on services like WhatsApp. If necessary he would go as far as banning the entire service (Griffin 2015; Jaffe and Zezima 2015).

The reaction of Cameron is the exact opposite of the view of how Verbeek thinks these technological developments should be treated. It also shows that to politicians the liberty of privacy becomes less important in the light of a perceived security threat. The public and the market are aware of this and are starting their own initiatives to protect their privacy. As Edward Snowden explains it in a recent "Ask Me Anything" chat on Reddit:

> The only way to ensure the human rights of citizens around the world are being respected in the digital realm, is to enforce them through systems and standards rather than policies and procedures (Snowden 2015).

With "systems and standards" Snowden is referring to privacy by design, a way to make it practically impossible for both the service providers themselves and third parties to listen in on private communications. This perspective conceptualizes privacy as material instead of theoretical. Paul M. Leonardi discusses three possible definitions of materiality. He defines matter as "related to physical substance", as "designating the practical aspect of something as opposed to the theoretical aspect" and as "having significance" (Leonardi 2010). The first two ways of looking at materiality will be discussed in its relation to the digital. Digital and

material will not be looked at as opposites, but as complementary characteristics that create their own affordances. In this thesis I will conceive of privacy as an entity that is always mediated by material means and only takes shape when people interact with materiality. Verbeek distinguishes two perspectives on mediation: a hermeneutic perspective which is concerned with the ways reality is presented to and can be interpreted by people, and a pragmatic perspective that approaches human-world relations from the human side and questions the ways in which people "act in their world and shape their existence" (Verbeek 2006b, 364-365). Here, I will use the hermeneutic approach in a focused material object analysis of WhatsApp and Telegram. More specifically, I will take a closer look at the mediation of privacy by design in these two mobile instant messaging services (MIM's).

First, I will investigate why privacy has become a topic of discussion in this era of big data. Secondly I will investigate how these points of discussion are reflected in the affordances of WhatsApp and Telegram. Thirdly, I will show how privacy is mediated in both services using Verbeeks theory of moral mediation, both on the level of the platforms and the level of corporate communication. Finally, I will argue that moral mediation, as described by Verbeek, lacks two features: It does not take into account that communication technologies often are accessible only as a black box (their true workings are hidden) and it does not appreciate the importance of existing power relations at its true value. As a combination these two features can problematize protection of human rights and ultimately, democracy. Therefore my main question will be:

> How do mobile messaging services WhatsApp and Telegram mediate privacy and how can this analysis enrich existing theory concerning the materiality of privacy in communication technologies?

To build my argument I will use the following sub questions:

1. How is privacy defined in an age of Big Data?
2. How are the characteristics of privacy and Big Data reflected in the design and affordances of WhatsApp and Telegram?
3. How can moral mediation be translated into a valuable methodology for the analysis of the materiality of privacy in communication technology?

2. Privacy in an Age of Big Data

I will investigate two terms that are central to the argument I intend to make. First, I will deal with both the popular and the academic perspective on Big Data systems. Secondly, I will explain privacy in terms of contextual integrity. The purpose of the investigation of these two definitions is to show how the characteristics of Big Data and contextual integrity are mutually exclusive. In the focused material object analysis of WhatsApp and Telegram I will show the ways in which these MIM's try to resolve the tension.

2.1 Big Data

In this day and age most electronic devices and systems collect information about how they are being used. Telephone companies record the specific time and duration of calls and the Dutch OV-chip card system records exactly from where to where someone travels each day (overview of the data landscape). The amounts of data that are being collected are huge and grow with each technological innovation. Most data collected now is not content but information about that content, called metadata. In the case of a mobile phone call this can be, amongst other information, call duration, time and date, location (GPS), phone number of receiver, IMEI nr. (the identification number of the phone that is used), etc. Because scope and volume is so vast the collected data has become inconceivable for humans. In the popular discourse the term used for these kinds of data systems is Big Data. The term Big Data can best be looked at in terms of a family resemblance as described by Wittgenstein (1958, 73): instead of one definition, using several possible characteristics proves to be more practical. The most comprehensive list of characteristics is posed by Rob Kitchin (2014a; 2014b). He combines the characteristics used in popular and industry discourse with the academic perspective on Big Data. Referring to Doug Laney (2001) and Chris Zikopoulos et al. (2012) he states that the most commonly used characteristics are the so called 3V's: volume, velocity and variety. Big Data can be "huge in volume", "high in velocity" and "diverse in variety" (Kitchin 2014a, 1; Kitchin 2014b, 68-78). Recent publications have suggested multiple additions to these characteristics. Referring to boyd and Crawford (2012) and Mayer-Schönberger and Cukier (2013), Kitchin (2014b, 68-78) describes Big Data as "exhaustive in scope", "fine-grained in resolution (...) and uniquely indexical in identification", "relational in nature" and "flexible (...) and scalable". These characteristics,

described in positive and even superlative terms, all have helped create the myth of Big Data.

When these characteristics are placed in an arena of public surveillance it becomes clear that collecting data about people can be very intrusive, even more when several databases from different spheres are linked. To conceptualize possible privacy harms I will borrow Helen Nissenbaums definition of privacy. In the next paragraph I will explain her framework of contextual integrity.

2.2 Privacy as Contextual Integrity

In her book *Privacy in Context: Technology, Policy and the Integrity of Social Life*, Helen Nissenbaum refers to political scientist Priscilla Regan to define privacy as a public value. This is important, since the value of privacy for the individual "is usually outweighed by countervailing social needs – dire or otherwise (e.g. business efficiency, national security, law enforcement, or economic prosperity)" (Nissenbaum 2009, 86). Regan explains three ways in which privacy supports democratic political systems, liberal democracies in particular. First, it supports the right of anonymous speech and freedom of association. Second, privacy protects people against agents of government, "particularly in spheres of life widely considered out of bounds" (Regan 1995, 226). Third Regan argues that privacy allows people to decide for themselves what distinguishing information or aspects about their lives they would like to share, in order to be able to emphasize their similarities with fellow citizens in public (Regan 1995, 227). Nissenbaum states that this state of affairs "affirms their equality as citizens; equal consideration is given to others and is expected in return" (Nissenbaum 2009, 86-87). In the continuing current of developing technologies Nissenbaum makes the observation that the perspective used to define contemporary privacy policies and law in the United States is not adequate to deal with issues of public surveillance. She recognizes three prevailing principles in that dominate public deliberation surrounding privacy:

> (1) [L]imiting surveillance of citizens and use of information about them by agents of government, (2) restricting access to sensitive, personal, or private information, and (3) curtailing intrusions into places deemed private or personal (Nissenbaum 2004, 107).

The first principle raises the question of where the limits of surveillance should be placed. If this limit only excludes places "deemed private or personal", public surveillance falls outside of the scope of these principles (Nissenbaum 2004, 116). When sensitive information is excluded, online surveillance in the form of online profiling is not part of this definition either. With the use of these three principles it seems as if public surveillance "is determined not to be a privacy problem" (Nissenbaum 2004, 116). Nissenbaum finds the solution to this counterintuitive notion by defining privacy in terms of integrity and placing it in its relevant context. She posits two types of informational norms: norms of appropriateness and norms of flow or distribution. Norms of appropriateness dictate "what information about persons is appropriate, or fitting, to reveal in a particular context" (Nissenbaum 2004, 120). For the definition of norms of distribution Nissenbaum draws upon the concept of complex equality as defined by Michael Walzer (1983):

> Walzer conceives of societies as made up of numerous distributive spheres, each defined by a social good internal to them. (…) These social goods are distributed according to criteria or principles that vary according to the spheres within which they operate (Nissenbaum 2004, 123).

Similar to these "social goods", information is always meant for a specific context and people should therefore be careful with its distribution. According to Nissenbaum complex equality "adds the idea of distributive principles to the notion of contextual integrity. What matters is not only whether information is appropriate for a given context, but whether its distribution (…) respects contextual norms of information flow" (Nissenbaum 2004, 123). In order to keep contextual integrity intact both informational norms have to remain intact. When one of the norms is breached, contextual integrity is violated. The possible privacy violations caused by the affordances of Big Data technologies as listed by Kitchin can easily be defined in terms of breaches of contextual integrity. Referring to Daniel Solove (2006), he lists several different ways in which privacy can be breached. Amongst these privacy breaches are "secondary use" and "appropriation". Secondary use is defined as information "collected for one purpose used for a different purpose without the data subject's consent" and appropriation is explained as "the use of the data subject's identity to serve the aims and interests of another" (Kitchin 2014b, 169). Both these possibilities are violations of the norms of distribution. In the next paragraphs I will investigate what affordances in relation

to privacy are present in the messaging services WhatsApp and Telegram as a result of Big Data technologies.

3. On Methodology

To be able to critically analyze moral mediation in MIM's, I will build a theoretical framework grounded in digital materialism as defined by Lev Manovich (2001). I will link affordance theory with digital metaphors and show how they affect the interrelations between affordance, design and appropriation. As my main structure I will use the five levels of digital media as defined by Nick Montford and Ian Bogost (2009). With this structure I will be able to perform a more focused material object analysis in which I will look exclusively at the affordances related to privacy and how these affordances are mediated, both by the design and the communications about the design. With this structure I will uncover the two weaknesses of Peter-Paul Verbeeks theory of moral mediation as mentioned in the introduction and offer a direction for a possible solution.

3.1 Digital Materialism

Although the digital and the material have often been presented as being opposites in the past, the current state of affairs in the digital humanities is that more and more the digital and material are investigated as being inseparable (Lehmann 2012). Code and digital programs are intangible, but they can only exist within a machine or computer and are therefore always "in-material", a term coined by Mirko Schäfer (2011, 63). Lev Manovich named the study and methods of digital objects within their material expression or appearance "digital materialism" in his book *THE LANGUAGE OF NEW MEDIA* (Manovich 2001, 35). In the field of game studies this perspective is used by Nick Montfort and Ian Bogost in *RACING THE BEAM*, a platform analysis of the Atari Video Game System (Montfort and Bogost 2009). They recognize five levels of digital media, which are reception/operation, interface, form/function, code and platform,

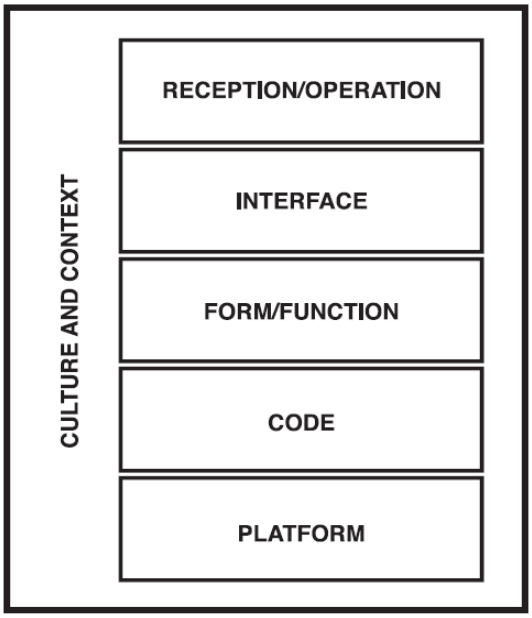


Image 1: The five levels of digital media, situated in context (Montfort and Bogost 2009, 146).

and place them within their culture and context (see figure 1). Montford and Bogost stress that most studies done in the field of new media usually focus on one of the levels, but are bound to take other levels into account as a result of overlap (Montfort and Bogost 2009, 146). To analyze the functionalities of the design and its materiality I will use the triad of affordance, design and appropriation as posed by Mirko Schäfer (2011, 20-21). This framework deals with material design and its relation to context and culture. The designs with their affordances are a result of the combination of all the five levels of digital media. The culture and context can be looked at in terms of appropriation, the way in which people use both the intended affordances and the unforseen affordances of a design (Schäfer 2011, 20).

3.2 Affordance Theory

Affordance is term made popular by ecological psychologist Gibson. He used the term for environments in relation to animals that lived there: "The affordances of the environment are what it offers the animal, what it provides or furnishes, either for good or ill" (Gibson 1979, 127). In a critical reading of Gibson's theory, ecological psychologist Anthony Chemero, explains the definition in the following way:

> An affordance, this seems to imply, is a resource that the environment offers any animal that has the capabilities to perceive and use it. As such, affordances are meaningful to animals: They provide opportunity for particular kinds of behavior. Thus, affordances are properties of the environment but taken relative to an animal (Chemero 2003, 182).

In science and technology studies the concept of affordance is used to analyze technologies in relation to humans. They also provide "opportunity for particular kinds of behavior", "either good or ill". As I will show in my analysis of WhatsApp, the choice to store unencrypted messages on a server creates the affordance of mass surveillance. The existence of this affordance does not necessarily mean that the opportunity is used, only that it is there. Ian Hutchby explains that the concept of affordance takes into account that artifacts both shape and are shaped by human practices. He states that "this third way, between the (constructivist) emphasis on the shaping power of human agency and the (realist) emphasis on the constraining power of technical capacities opens the way for new analysis of how technological artifacts become important elements in the patterns of ordinary human conduct" (Hutchby 2001, 444). In this case the "constraining power of

technical capacities" will be important in particular, since (physical) constraints "are closely related with real affordances" (Norman 1999, 40). For example, Telegram messages are not stored on servers and are encrypted in the process of sending. These characteristics afford safe communications.

Bruno Latour also recognizes that technological objects should be studied within their context, or as he explains it: "[w]e are to follow the simultaneous production of a 'text' and a 'context'" (Latour 1991, 106). When affordances and constraints are placed in the context of human conduct they are able to carry certain politics (Winner 1986; Latour 1991, 103-132). Bruno Latour showed that a message or policy can be translated in an object. As an example he used the weights attached to hotel room keys, which translate the message "leave your hotel room keys at the lobby" (Latour 1991). Both material and (digital) in-material objects are able to carry these kinds of messages, but as I will explain in the next paragraph, digital affordances are in most cases obscured by metaphors.

3.3 Metaphors

The interface of a computer translates human language and instructions into code. Marianne van den Boomen reads these translations as metaphors, since the signs used are most often representations of things in the material world (van den Boomen 2014). A digital button on a screen for example, merely executes certain code when it is 'pressed', instead of its physical counterpart that mechanically activates a function of a machine. This obscurity is not only reserved to the inner workings of digital objects, but is equally present in mechanical devices as Albert Borgmann points out:

> A simple phonograph produces poor sound. Correspondingly, today's stereo, which produces preternaturally perfect sound, is totally unintelligible to the typical consumer who does not even begin to understand the mathematics, logic, electronics, and mechanics that are embodied in a compact disc player and its associated equipment. As a consequence music has become a disembodied, freefloating something, a commodity that is instantly, ubiquitously, and easily available (Borgmann 1992, 296).

The compact disc player functions as a black box and has turned music into a commodity. In the digital domain similar processes are at work in interfaces of computers and

smartphones. Van den Boomen explains that digital interfaces are even further away from their inner workings:

> The metaphorical and the symbolical representations on the screen provide the user with an interface that enables operating the machine, yet at the same time it channels attention away from the machinery (van den Boomen 2014, 15).

The metaphorical symbols used in the interface are able to refer to a (slightly) different practice than the one they are signifying. In WhatsApp for example, the word privacy only signifies three possible contexts for sharing information. In this sense privacy becomes a metaphor for three options in the application. Privacy in relation to surveillance is actively depresented both in the interface and in the company's communications. This requires a certain attitude from its users:

> Reading and using these interface metaphors requires a precarious balance between, on the one hand, being able to recognize their compressed metaphoricity that stands in for a complex dynamic machinery, and on the other hand, being able to forget this, that is, reify the metaphor and take it as a thing in itself (van den Boomen 2014, 14-15).

When artifacts have politics, but are at the same time using metaphors obscuring their workings, and thus their politics, it becomes harder for users to keep the balance Van den Boomen is referring to. The way to go, according to philosopher Peter-Paul Verbeek, is to actively engage with technologies in order to guide them in a preferred direction (Verbeek 2014). In the next paragraph I will explain how this is placed in Verbeeks theory of moral mediation.

3.4 Moral Mediation

For the inbuilt politics of technologies Peter-Paul Verbeek borrows the term 'technological intentionality' from Don Ihde (1990) in order to build his own theory of moral mediation (Verbeek 2006a; 2007; 2013; 2014). He states that people have to learn how to deal with technological intentionality. They should learn how to spot intentions and "permit them in a critical and creative way" (Verbeek 2014, 154).[1] The concept of moral mediation as defined by Verbeek is based on the principle that humans and non-humans can possess moral agency. As a result, technological design becomes a "crucial ethical activity, albeit by other

[1] All citations from Peter-Paul Verbeeks *OP DE VLEUGELS VAN ICARUS* (2014) are translated from Dutch by me

means" (Verbeek 2014, 49). His emphasis shifts therefore from a theoretical to a practical application of ethics:

> Designers materialize morality. Ethics is no longer done exclusively based on philosophical reflection, but also on practical experiment, in which the subjective and the objective, the human and the non-human are interwoven (Verbeek 2014, 49).

At first sight it might seem counterintuitive to permit artifacts in the domain of moral agency, since free will and the freedom to act upon this will, seem prerequisites for any intentionality. Instead of rendering moral agency for artifacts impossible, Verbeek chooses to redefine freedom itself. He states that freedom is "not the absence of limitations and influences, but the relation with them" (Verbeek 2014, 75). Since technologies are mediating this relation, they actively shape morality.

Within technological mediation Verbeek recognizes three levels: seducing, persuasive and forcing technologies (Verbeek 2014, 104). For example, in order make people slow down their cars in a school area, a seductive design would be a road sign asking motorists to slow down. A speed camera would be a more persuasive technology, increasing the incentive to slow down, but still leaving choice to drive fast open. A speed bump could be seen as a forcing technology, since driving too fast without damaging ones car is made impossible. In Latours terminology all three technologies can be seen as a translation of the phrase "slow down". When these technologies become a part of our lives, moral acts and decisions have become a hybrid affair of both humans and technology (Verbeek 2014, 134). According to Verbeek, mediation theory makes it possible to look beyond intended and unintended effects of technologies and not only "evaluate new technologies in terms of the quality of their functioning (…), but also in terms of the way they help shape new experiences and practices" (Verbeek 2014, 138). As a model for reflection, he uses a rather linear approach to the relationship between designer, technology and its user without any feedback (see image 2).

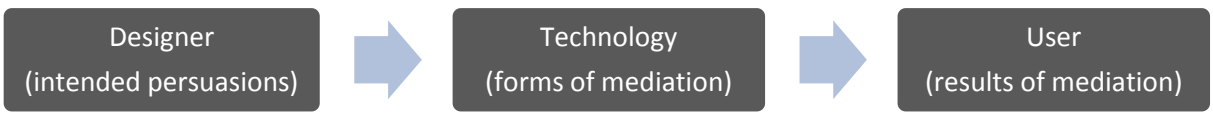


Image 2: Model for ethical reflection in the design of persuasive technology as shown in Verbeek (2014, 139)

This has its effect on the way Verbeek conceptualizes the technologically mediated moral subject. Instead of resisting unwanted effects people should uphold an attitude of releasement as defined by Heidegger. He places this attitude in contrast with what he calls "a popular reading of Foucault" (Verbeek 2011, 71; 2014, 89). As an illustration of this popular reading Verbeek cites Jana Sawicki:

> Freedom lies not in the discovery of essential features of the human situation, in complete mastery of reality or in releasement"; it rather lies in the relations people develop toward the "dominating powers of technology (Sawicki 2003, 69 as cited in Verbeek 2011, 71).

Resisting these "dominating powers of technology" would not create a realistic alternative. The only use for a dialectic perspective in this situation is, according to Verbeek, to show that each antiposition can only be defined in terms of the position it aims to resist. Instead we should aim for a synthesis, resulting in a sublation, in order to go beyond resistance (Verbeek 2011, 72). As I will show with following case studies, such a synthesis seems rather unfeasible. Resisting is hard when daily communication technologies are mediating privacy via the use of metaphors, and are used as technologies of government surveillance. Yet, an attitude of releasement seems impossible, or maybe even counterproductive.

4. A Case Study: WhatsApp and Telegram

In the following case study I will discuss affordance, design and appropriation in mobile instant messaging apps WhatsApp and Telegram. WhatsApp is currently the most popular MIM in the world with 600 million active users (Olson 2014). I choose Telegram because its functionalities are very similar to WhatsApp, but in the "Secure Messaging Scorecard" of the Electronic Frontier Foundation (EFF), an organization occupied with defending civil liberties in the digital world, the *secret chat* function of Telegram is awarded with all seven checkmarks (as opposed to WhatsApp's two checkmarks) (Electronic Frontier Foundation 2015). The EFF tests messaging apps on End-to-End encryption, if messages are encrypted for their provider, possibilities to verify contacts identities, if past communications are secure in the case of stolen keys, if the code is open to independent review, if the security design is properly documented and if there has been a recent security audit. Whenever I refer to Telegram from now on, I will be referring to the secret chat function of this

messaging service. After introducing both applications and the people that created them I will analyze how they mediate privacy using the framework of Montford and Bogost (2009).

4.1 WhatsApp: Simple. Personal. Real Time Messaging

WhatsApp Inc. was founded in 2009 by two former employees of Yahoo! Inc., Brain Acton and Jan Koum (Jackson 2014). The name WhatsApp is derived from wordplay on the phrase "what's up" (WhatsApp 2015a). According to the creators the incentive to start creating WhatsApp came from a wish for privacy:

> These days companies know literally everything about you, your friends, your interests, and they use it all to sell ads. (...) [W]e wanted to make something that wasn't just another ad clearinghouse. We wanted to spend our time building a service people wanted to use because it worked and saved them money and made their lives better in a small way (WhatsApp 2015c).

This view on business worked quite well and WhatsApp is currently the most popular MIM in the world with 600 million active users (Olson 2014). On the secure messaging scorecard of the EFF it scores only two out of seven checkmarks: one for encryption in transit and one for a recent code audit. In the rest of the analysis I will not only show the reasons for this rating of the affordances and design of WhatsApp, but also the way in which the company communicates these affordances and its design.

4.2 Telegram: Taking Back Your Right to Privacy

One of the few electronic communications that score all seven checkmarks by the EFF is the secret messaging function of Telegram (Electronic Frontier Foundation 2015). Telegram was launched in 2013 by two brothers, Nikolai and Pavel Durov, founders of VKontakte, Russia's most popular social network site (Shu 2013). It is actively marketed as a response to WhatsApp as one of the questions in their Frequently Asked Questions (FAQ) is even "How is Telegram different from Whatsapp" (Telegram 2015e). The creators emphasize that they have no commercial interests, but rather see Telegram as an ideological project:

> Telegram is a noncommercial project with an aim to create a truly free messenger, without the usual caveats. This means that instead of diverting attention with low-impact settings,

we can afford to focus on the real privacy issues that exist in the modern world (Telegram 2015f).

This statement shows they intend to make privacy an issue, both in the affordances of their product and in the way these affordances are communicated in their product.

4.3 Platform

The platform of an application can refer to both the device and the operating system it can be used on. WhatsApp and Telegram can both be used on all smartphones running on Android, iOS or Windows. In addition to these, WhatsApp also works on Nokia S40, Nokia S60, BlackBerry and BlackBerry 10. The latest addition is a web version of WhatsApp which makes it possible to use the messenger in all internet browsers. Telegram is available for Firefox OS on mobile devices and has a web version and Chrome app. In addition to that, there is a desktop app for Windows, Linux, Mac and Mac OS X. Because of constraints on time and words, in the remaining part of the analysis I will only discuss the Android app of both services. This is the most used operating system on mobile phones with a market share of more than 70 percent (Edwards 2014). Moreover, the design and affordances of this version are similar to the iOS and Windows apps.

A feature of mobile phone platforms is the so called “push notification”. When a message arrives the user of the phone will be notified of this, even when the application is not opened in the phone. This notification can have multiple forms. Depending on the settings of the operating system the phone can play a sound, vibrate and show a (part of the) message in the screen. In Android an icon will appear in the upper left of the screen (see image 3). When the notification is opened details become visible. A notification of a WhatsApp message will show the profile picture and name of the sender, the time and number of messages and (a part of) the message itself (see image 4). A telegram notification contains less information by default (this can be changed in the settings): only the time and number of messages. The name of the sender and content of the message are only visible when the application is opened.

Image 3: The WhatsApp and Telegram notification symbols in the top left corner of the screen

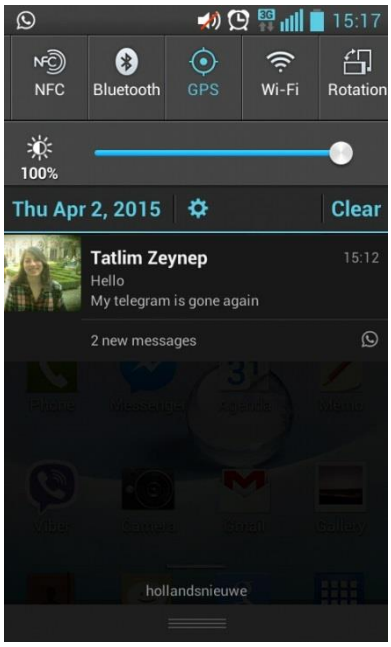


Image 4: A WhatsApp notification showing the name of the sender, profile picture, number of messages, time and (part of) the message.

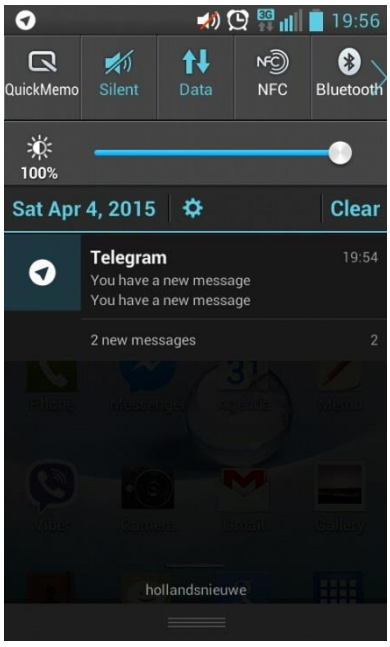


Image 5: A Telegram notification showing only the time and number of messages. The content is replaced with "You have a new message".

4.4 Code

Although looking into the source code of both apps goes beyond the scope, timeframe and expertise of the writer of this thesis, information can be gained from the manner in which both companies communicate their inner workings. On the "open source" page of their website, WhatsApp refers to the fact that it is developed using open source software "from the early days" (WhatsApp 2015b). They continue to state that "WhatsApp engineers use, contribute to and release a lot of open source software" (WhatsApp 2015b). On the bottom of the page several open source programming languages and structures are listed. However, the way in which they are used, if they are still used, remains unclear, since the source code of WhatsApp itself is not open. The WhatsApp Application Programming Interface (API), a way for programs to interact with each other, only offers the possibility to open a chat or exchange files.

Telegram also makes use of open source programming languages and offers a partial source code of their applications on their website. They state that they focus on "open sourcing the things that allow developers to quickly build something using our API" and that they "will be releasing more code eventually" (Telegram 2015d). In another page on the website Telegram explains the encryption technology it uses in detail (Telegram 2015b). It might seem like they

offer a lot of information to possible code breakers. However, the fact that they offer a reward of $200,000 (later increased to $300,000) to the first person that is able to break their encryption shows that they are quite confident their privacy by design will withstand rigorous tests (BBC News 2013). As of April 10, 2015 this reward has not been claimed by anyone (Telegram 2014b).

4.5 Form/Function

When Montford and Bogost refer to the form and function of a digital object, they think of these concepts in relation to computer games. The form and function of these digital objects are looked at in terms of narrative and "rules of the game" in order to analyze the core of the program (Montfort and Bogost 2009, 146-147). In the case of MIM's I will translate this notion of form and function to the way in which the apps treat information and the way in which this is communicated. I will discuss the visual mediation of form and function of the inner workings of WhatsApp and Telegram in the next section about the interface. The three types of information I will discuss are contact information, message metadata and the message content.

4.5.1 Contact Information

Both WhatsApp and Telegram handle contact information locally, which means that they only acquire the phone numbers of the contacts of a user. Extra information is not transferred to their servers. WhatsApp states the following in their privacy statement:

> WhatsApp does not collect names, emails, addresses or other contact information from its users' mobile address book or contact lists other than mobile phone numbers—the WhatsApp mobile application will associate whatever name the WhatsApp user has assigned to the mobile telephone number in his/her mobile address book or contact list — and this occurs dynamically on the mobile device itself and not on WhatsApp's servers and is not transmitted to WhatsApp (WhatsApp 2012).

This statement only addresses information outside of the WhatsApp application. The information users share about themselves within WhatsApp, such as a profile picture, status (a statement of less than one sentence which can address everything from mood to a recent experience) and online/offline status, are not part of this statement. Within WhatsApp, users can choose from three options to show their profile picture, status and last seen time: "everyone", "only contacts" and "nobody". Telegram handles contact information in a

similar way to WhatsApp and even offers the option to create a username to which people can send messages without them finding out your mobile phone number (Telegram 2015e). How information is shared within the application is up to the user. Instead of three predefined categories, users can include or exclude specific contacts from information at their own will (Telegram 2014a).

4.5.2 Metadata

Communications via MIM's also create the possibilities for the collection of metadata. Metadata in this case could be anything related to the message other than the content itself such as time, location (acquired via GPS) and phone numbers. WhatsApp does collect metadata of sent messages:

> WhatsApp may retain date and time stamp information associated with successfully delivered messages and the mobile phone numbers involved in the messages, as well as any other information which WhatsApp is legally compelled to collect (WhatsApp 2012).

What WhatsApp is "legally compelled to collect" is not explained anywhere. Telegram on the other hand does not discuss metadata anywhere in their FAQ and privacy statement.

4.5.3 Content

Instead of metadata Telegram focusses on the content of the messages and state that they use "end-to-end encryption" (Telegram 2015c). This means that in a secure message the content is encrypted in the phone of the sender, then travels encrypted through the servers of Telegram and is decrypted in the phone of the receiver. With this approach it is impossible for a third party to gain access to messages not intended for them. Even if a government where to request the content of a secure message, Telegram itself would not be able to give it. Another factor that complicates possible spying on Telegram secret chats more difficult is the fact that they only travel through the servers and never stay there, since messages are only sent when both the sender and receiver are online. If either one of them is offline the message will stay on the phone of the sender. A WhatsApp message will be send to the server and stay there until it can be delivered. This offers more flexibility in connectivity but is also a possible security risk.

WhatsApp is both less secure and less outspoken about their encryption. In their FAQ they explain that messages are encrypted "between your phone and our server" (WhatsApp

Support Team 2015). This means, although it is not explicitly stated, that on the server of WhatsApp messages are plain text, pictures and sounds, which in turn means that WhatsApp itself and possibly governments are able to access them. About the archiving of messages that travel through their servers WhatsApp states the following:

> The contents of messages that have been delivered by the WhatsApp Service are not copied, kept or archived by WhatsApp in the normal course of business (WhatsApp 2012).

Just as the information they are "legally compelled to collect", the "normal course of business" is a vague term that can be interpreted very broadly. Instead of worrying about this possible privacy threat, WhatsApp warns users for the possibility of others reading your messages when they have physical access to your phone (WhatsApp Support Team 2015). Telegram addresses this problem by offering the possibility of securing the application with a passcode (see image 6) (Telegram 2015e). Since the push notifications do not show any content either, no information can be accessed by anyone that does not have the passcode of the application.

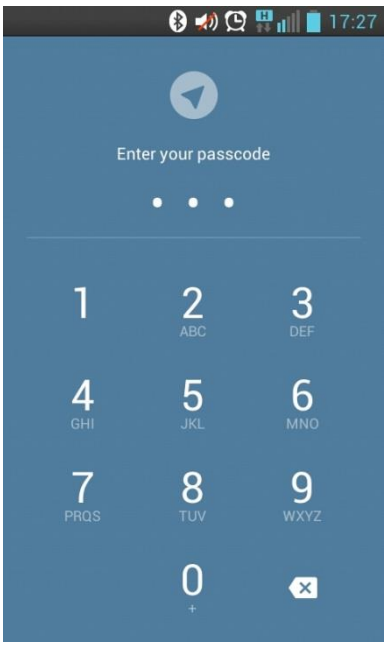


Image 6: Telegram passcode screen

4.6 Interface

The first thing a user encounters when both Telegram (after the passcode if applicable) and WhatsApp are started is a list of all ongoing communications (called 'conversations') with other contacts. The most recent conversations are on top and the oldest, if not removed, are on the bottom (see image 7). When the options button is pressed (where this is located differs from device to device) in either of the apps a menu opens showing all the options of the app. In WhatsApp there is only one type (as far as security goes) of message (image 8). In Telegram the default is a "secret chat" (image 9), however when a conversation is started from the contacts menu a normal chat is opened. In both WhatsApp and Telegrams settings menu privacy settings can be found.

Image 7: WhatsApp conversations listed from most recent to less recent

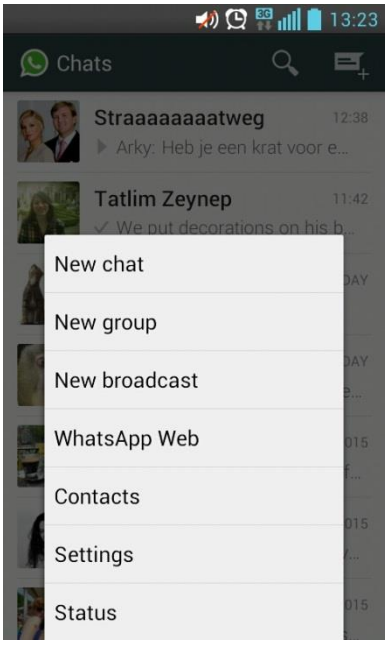


Image 8: WhatsApp options menu

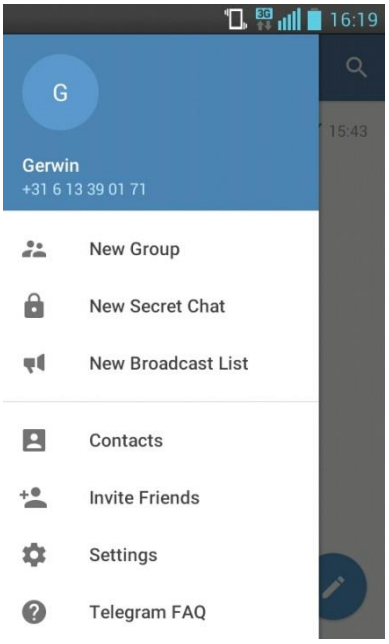


Image 9: Telegram options menu.

In Telegram it is called the Privacy and Security menu (see image 10). In WhatsApp the 'privacy settings' (see image 11) only offer three predefined options for sharing: "everyone", "my contacts" and "Nobody" (see image 12).

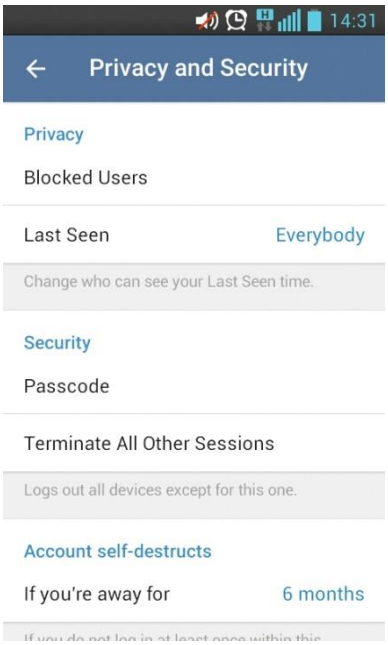


Image 10: Privacy and security settings of Telegram

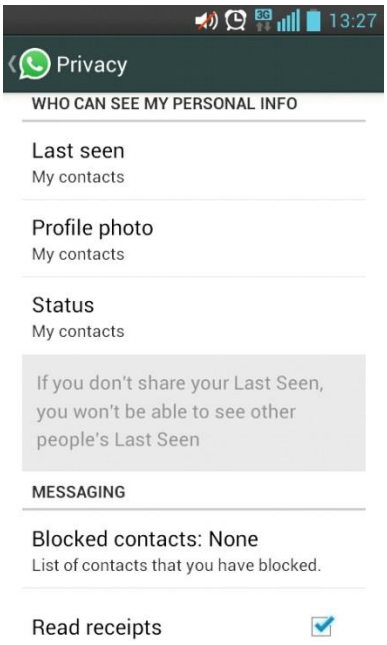


Image 11: Privacy settings of WhatsApp

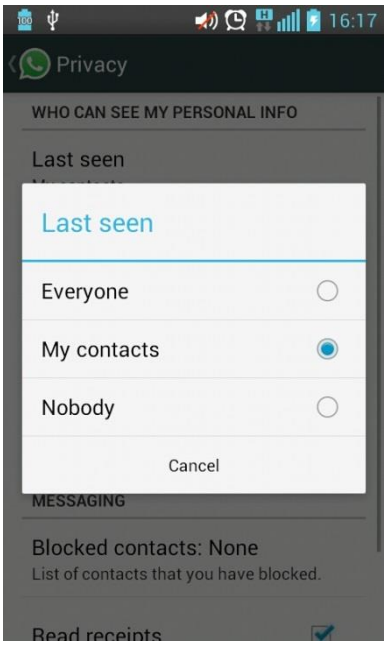


Image 12: Three predefined options in the privacy settings of WhatsApp

In a conversation the most recent messages are added on the bottom in order to create a conversation that can be read from top to bottom. Both MIM's offer indicators for the arrival status of messages in the form of checkmarks, but do this in a slightly different way. In

WhatsApp a message will show one checkmark when it has reached the server, two checkmarks when it has reached the phone of the receiver and the checkmarks will turn blue when the receiver has opened the conversation (see image 13). In a Telegram secret chat conversation a message has either no checkmarks meaning the recipient is or has not been online yet, or two checkmarks meaning that the recipient has the conversation opened in his phone and received the message (see image 14).

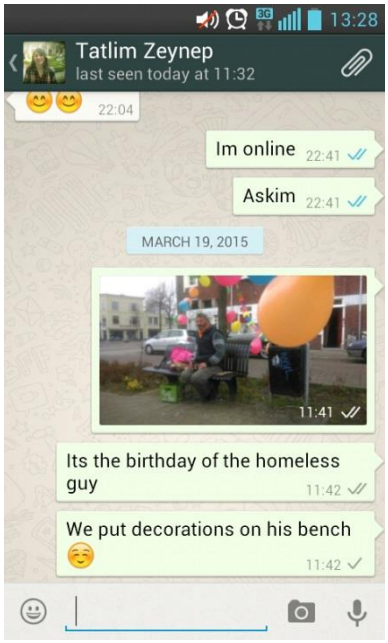


Image 13: WhatsApp conversation with checkmarks (right) indicating the arrival status of the messages.

Image 14: Telegram secret chat conversation with checkmarks indicating the arrival status of messages.

Above a conversation, the name of the contact (as it is listed in the phone) is shown and the last time this person opened WhatsApp or Telegram (this is only visible when the other person is allowed to see the same information). Next to the contacts name is an icon that, when tapped on offers more options. In WhatsApp the icon is a paperclip which offers the possibility to attach different digital objects to messages: a picture, photo, sound, video, location information or contact information (see image 15). When the name of the contact itself is tapped a contact

Image 15: WhatsApp message options for attachments are adding a picture, photo, video, sound, location and contact.

Image 16: Telegram secret message options are setting a self-destruct timer, clearing history, deleting a chat and muting notifications.

information menu opens. This menu offers some extra information about the contact and previously sent pictures (see image 17). In Telegram this menu offers some extra options for a specific conversation (see image 18). A self-destruct timer will delete messages after a set time. It also offers a visualization of the encryption key (see image 19). To be completely sure messages are secure it is possible to compare the keys with a contact. Only if they are exactly the same the encryption is effective. I will elaborate further on the relevance of self-destruct timer and the visualization of the encryption key in the next section.

The attachment option (also signified with a paperclip sign) is located in the bar where the message is typed. In the top of the screen there are three dots that, when tapped, give four totally different options (see image 16). The first one is a self-destruct timer, which when activated, will make each message that is sent disappear after a specific amount of time. The clear history option will delete all the previous messages, on all the devices the conversation is on, including the ones owned by the receiver. By deleting a chat the whole conversation will be erased on both the contacts devices. Muting notifications means that no sound will be played and the phone will not vibrate when a message is available.

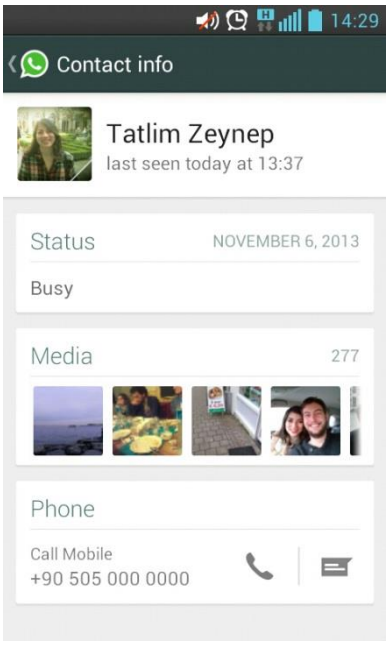


Image 17: Contact information in WhatsApp

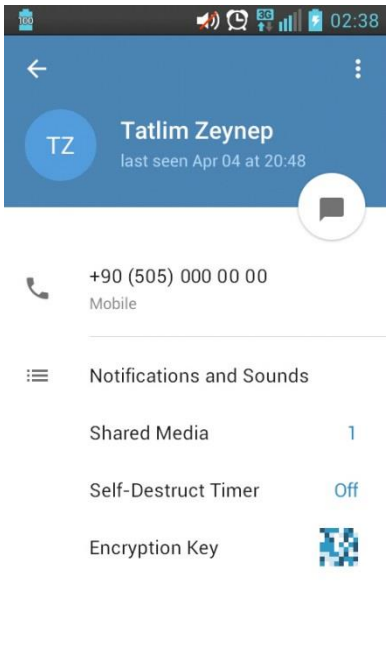


Image 18: Conversation information in Telegram

Image 19: Visualization of an encryption key of a secret message in Telegram.

4.7 Reception/Operation

Several recent events have shown that reception and operation of WhatsApp has a close relationship with the reception and operation of Telegram. In this part of the analysis will not only focus on the reception or operation by consumers but also by the companies themselves and governments. Consumers use MIM's to communicate with each other. WhatsApp offers an application for commercial use, which results in the fact that privacy is not their first concern. This can be read in their privacy statement:

> WhatsApp uses commercially reasonable physical, managerial, and technical safeguards to preserve the integrity and security of your personal information. We cannot, however, ensure or warrant the security of any information you transmit to WhatsApp and you do so at your own risk. Using unsecured Wi-Fi or other unprotected networks to submit messages through the WhatsApp Service is never recommended. Once we receive your transmission of information, WhatsApp makes commercially reasonable efforts to ensure the security of our systems (WhatsApp 2012).

How far these "commercially reasonable physical, managerial, and technical safeguards" and "commercially reasonable efforts" go is not mentioned. The creators of Telegram on the other hand clearly have an ideological incentive:

> Big internet companies like Facebook or Google have effectively hijacked the privacy discourse in the recent years. Their marketers managed to convince the public that the most important things about privacy are superficial tools that allow hiding your online status, your public posts or your profile pictures from the people around you. (…) At Telegram we think that the two most important components of internet privacy should be instead:
>
> 1. Protecting your private conversations from snooping third parties, such as officials, employers, etc.
> 2. Protecting your personal data from third parties, such as marketers, advertisers, etc. (Telegram 2015f)

They actively communicate that privacy is their first concern and show that, since they are a foundation, they have no commercial interests. The operation of WhatsApp also differs from Telegram. Where WhatsApp does not represent certain contexts and only asks from the user to take care of their physical privacy, basically leaving the rest to them, Telegram makes the users themselves part of the privacy verification process by means of the visualization of the

encryption key. The self-destruct timer also gives users more control over their messages. The fact that deleting a message will result in the removal of the message on all devices makes sure that everyone remains in control over their communications even after they have been sent.

The number of users of Telegram and WhatsApp does not reflect a particular concern for privacy. Even after the revelations of Snowden people are either indifferent or feel like they have to use WhatsApp because everyone else does. However people do worry about how much information several big companies have about them. The following passage of the privacy statement of WhatsApp deals with this problem:

> In the event that WhatsApp is acquired by or merged with a third party entity, we reserve the right to transfer or assign the information we have collected from our users as part of such merger, acquisition, sale, or other change of control. In the (hopefully) unlikely event of our bankruptcy, insolvency, reorganization, receivership, or assignment for the benefit of creditors, or the application of laws or equitable principles affecting creditors' rights generally, we may not be able to control how your personal information is treated, transferred, or used (WhatsApp 2012).

The relevance of this passage was shown when in February 2014 WhatsApp was acquired by Facebook and people started flocking to Telegram (Zuckerberg 2014; Tsotsis 2014). Too much information within one organization apparently does concern people.

4.8 Culture/Context

Facebook has, amongst other big IT companies, a direct connection with the NSA (Greenwald 2014, paragraph 229-230). It could therefore be expected that a similar connection now exists with WhatsApp. However, WhatsApp is still partly autonomous and they decided to start working with encryption start-up Whisper Systems. This led to several far reaching statements by leaders of the United States and the United Kingdom. Barack Obama, president of the United States, suggested that the government should have a ‘backdoor’ (Oremus 2015). David Cameron, Prime Minister of the United Kingdom, even went as far as threatening to ban WhatsApp if it was not accessible by security agencies (Griffin 2015; Jaffe and Zezima 2015). These reactions show that the government is expecting to be able to use popular communication technologies for public surveillance.

The governments seem less concerned with WhatsApp alternatives such as Telegram, although an important reason for this might be the number of users and the number of messages both applications deal with. However, Telegram does not have a commercial incentive and clearly also tries to propel the discussion about privacy. Interestingly they do not only do this by public statements or their frequently asked questions, but also by mediating the affordances of their application in such a way that users are made a part of the privacy process. WhatsApp, on the other hand, chooses not to communicate the affordances of their app (and thus the possibility of surveillance) in their interface.

5. Technologically Mediated Privacy

The designs of both WhatsApp and Telegram offer affordances that mediate privacy in different ways. Here I will discuss these affordances on two levels: a material level and an in-material level. Together these levels give a picture of how either company translates privacy through their technology.

WhatsApp emphasizes the importance of physical privacy. People should make sure no one is looking over their shoulders and that they are have a safe Wi-Fi connection (WhatsApp 2012; WhatsApp Support Team 2015). However, their design does not contain any physical barriers. When someone else is able to access a phone with WhatsApp, all notifications can be read and the application, with all the conversations, can be opened without any problem. The security of the messages is therefore the responsibility of the owner and user of the phone. Both on the material and the in-material level WhatsApp makes “commercially reasonable efforts” to make sure that messages remain private. In their design messages are only encrypted when they are travelling between a phone and their server, not on the server itself. This creates the affordance for WhatsApp, and therefore government agencies, to look into, and record the messages sent. However, this affordance remains invisible in the user interface and concealed in clever use of language in the company’s communications. The privacy settings in WhatsApp function as a metaphor for a very limited form of contextual integrity. The only possible contexts to choose from are “everyone”, “my contacts” and “nobody”. These are the only contexts in which a user can decide over their norms of appropriateness and distribution. The company WhatsApp and the NSA are two contexts that are left out of the both the interface and the communication of the company. How they

are able to handle personal data is not mentioned or translated into an affordance of the app. With regard to the security of messages, WhatsApp functions as a black box. Instead of making the inner workings visible WhatsApp keeps on warning for third parties, not including themselves or government agencies.

Telegram has privacy as their main goal. They employ several material privacy features. Telegram notifications cannot be read by default when the application is not opened and the application itself can be secured with a passcode. These options do not require a lot of technological understanding of the applications, but are easy switches in the interface. The transmission of messages is secured by end-to-end encryption, meaning that messages are encrypted on the phone of the sender, stay encrypted when they travel through the servers of Telegram and are decrypted on the phone of the receiver. This results in the fact that not even Telegram, let alone any government agency, is able to look into communications. By not including this affordance in their design they make an active choice for privacy and let the users of the app decide over their own norms of appropriateness and distribution. Ironically, Telegram tries to communicate its inner workings and partially open up the black box, by offering a visualization of the encryption key of a conversation. By comparing the visualization of the encryption keys of a message, the user becomes a part of the verification process. In this way some agency and responsibility concerning privacy is given back to the user. How this visualization, a metaphorical representation of the actual encryption key, is generated remains unclear for the layman. Telegram does offer a more detailed explanation of their code in the “FAQ for the technically inclined” (Telegram 2015a). The privacy and security settings of Telegram also reflect a more nuanced understanding of privacy. The users have control over all contexts and can include or exclude people at their own will (instead of three predefined settings). The secret chat has an important place in the design of Telegram. The creators could have chosen to make all conversations “secret” by default, but that would have meant that Telegram would look and operate the same as WhatsApp, only promising more privacy. In order to make privacy a topic of discussion, Telegram has made it a visible working part of their application. They have taken privacy out of the black box and placed it in the forefront of the public debate.

After Snowdens revelations privacy has become widely discussed topic in the popular discourse. The market has responded with a lot of technologies that are able to better

ensure the privacy of their consumers. Analyzing these applications through the framework of moral mediation reveals its limitations. By using a rather linear approach to the relationship between designer, technology and user it might seem like the production of meaning is a one way street and has only room for one interpretation. Who is the user in this approach? The case studies show that different groups of people have different incentives with the technologies at hand. WhatsApp tries to make money, people want to communicate easily and privately and the government would like to ensure the safety of the nation (the question if surveillance of MIM's is an effective strategy to achieve this is beyond the scope of this thesis).

The Electronic Frontier Foundation is trying to make the big public aware of the differences in the way WhatsApp and Telegram, amongst other communication applications, mediate privacy. However its message is somewhat ambiguous. John Perry Barlow, one of the cofounders of the EFF, once famously wrote the following in his "Declaration of Independence of Cyberspace":

> Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here (Barlow 1996).

This statement suggests that the internet is not material, which in turn only obscures the affordances it might create. Frederick Turner correctly acknowledges that the notion that cyberspace is "a place apart from the ordinary material world", makes it harder to see that the internet depends on "real, material networks of cables and switches, antennae and satellites" for its existence (Turner 1999, 10). The electronic frontier metaphor "renders the power of infrastructure owner invisible, it makes it that much harder for individual internet users to challenge that power" (Turner 1999, 10). Challenging this power now happens mainly between the players in the market. In the discussion around privacy, Telegram is actively attacking WhatsApp both in their FAQ and their public statements. Verbeek does not favor such an attitude since resistance is only defined through the power it is resisting (Verbeek 2011, 90). Rather people should actively engage with technologies and guide them. In order for this to work, an attitude of releasement is needed. However, it remains unclear what such an attitude should encompass. How can people actively engage with and guide

technologies when their inner workings are hidden? One statement made by Nissenbaum in a pre-Snowden era is revealing:

> My purpose here has not been to settle the question but to reveal a potential connection between unbridled data collection, aggregation, and profiling and a subtle erosion of autonomy. As far as I can see, there is insufficient evidence to claim that these systems and practices, in general, lead to coercion, deception, and manipulation, only that they may (Nissenbaum 2009, 84).

We now know that "unbridled data collection, aggregation and profiling" provide the affordance for "coercion, deception and manipulation". Instead of simply assuming that companies and governments will behave ethically, or even according to their own laws and regulations, from now on privacy should be incorporated in the structure of the technologies used. To strengthen this argument I would like to come back a statement by Edward Snowden used earlier:

> The only way to ensure the human rights of citizens around the world are being respected in the digital realm, is to enforce them through systems and standards rather than policies and procedures (Snowden 2015).

Morals have always been incorporated in material culture. Andrew Feenberg acknowledges this when he discusses what he calls technological rationality:

> [T]echnological rationality is not merely a belief, an ideology, but is effectively incorporated into the structure of machines. Machine design mirrors back the social factors operative in the prevailing rationality. The fact that the argument for the social relativity of modern technology originated in a Marxist context has obscured its most radical implications. We are not dealing here with a mere critique of the property system, but have extended the force of that critique down into the technical 'base'. This approach goes well beyond economic distinction between capitalism and socialism, market and plan. Instead one arrives at a very different distinction between societies in which power rests on the technical mediation of social activities and those that democratize technical control and, correspondingly, technological design (Feenberg 1992, 310-311).

In this neo-Marxist approach Feenberg explains the "technical mediation of social activities" as an instrument in protecting and reinforcing the powers that are in place in society.

However, the power reinforcing possibilities that are available in technological designs do not have to be placed in there intentionally. The concept of moral mediation is not able to recognize and evaluate instances of appropriation. Therefore it needs to be expanded. The consequences of a society in which the power rests on the technical mediation of social activities are stressed by Snowden in the documentary *CITIZENFOUR*:

> The balance of power between the citizenry and the government is becoming that of the 'ruling' and the 'ruled' as opposed to (...) 'the elected' and 'the electorate' (Edward Snowden in Poitras 2014).

To be able to democratize the technical control a system of privacy by design is needed. To be clear, I am not trying to force this analysis into a dialectical model of power relations. Rather, I would like to show that a theory dealing with the morality of artifacts should have room for multiple interpretations of an object and should be able to deal with (partially) hidden affordances. An interpretation of the allegory of Icarus by Pieter Bruegel de Oude shows the results these problems: no one seems to notice how technology is failing (see image 20). While Icarus has fallen from the sky, the working class simply continues with their daily tasks. The fisherman keeps on fishing and the farmer keeps on plowing his land. The shepherd is just dreaming away, while he gazes at the sky.

Image 20: De val van Icarus (The Fall of Icarus) by Pieter Bruegel de Oude (ca. 1558)

6. Revisiting Moral Mediation

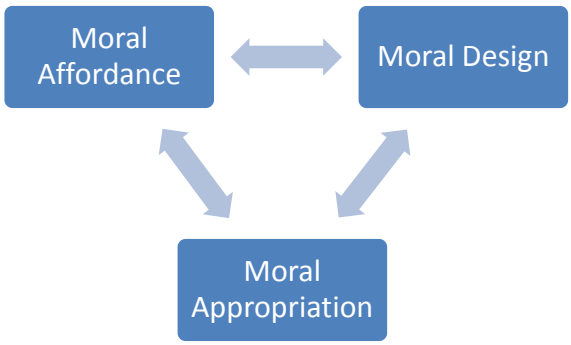


Image 21: Triad of moral affordance, moral design and moral appropriation

Because of constraints in time and space it will be impossible to build a complete theoretical framework from the bottom up. Instead I will give a general outline of how a methodology for the analysis of the materiality of privacy in communication technology could be constructed. To counter the problem of the linearity of the relationship between designer, technology and user, I will construct a theoretical framework based on Mirko Schäfers triad of affordance, design and appropriation (Schäfer 2011, 20-21). Taking affordances into account, this theory goes further than the functionalities intended by designers. Appropriation gives room to multiple interpretations of technologies by more than one type of user. I therefore propose to add a moral dimension to Schäfers triad, creating a triad of moral affordance, moral design and moral appropriation (see image 21). With this framework two problems of the theory of moral mediation can be countered. First, moral design offers a place for the analysis of the metaphoricity of digital objects. By analyzing the metaphorical and symbolical representations in the moral design of digital artefacts using the theory of Van den Boomen (2014), hidden moral affordances come to the surface. These metaphors can work on all the levels (not just in the interface) recognized by Montford and Bogost (2009). A detailed analysis, taking all the levels into account is therefore vital. Second, moral appropriation leaves room for multiple, moral interpretations of a technology. The definition of a user in this model can encompass much more than just the classical consumer or member of the big public. In this model, the companies offering a technology or government agencies using it for surveillance, can also be defined as moral appropriators of a technology. When moral mediation is placed within moral appropriation it can work in multiple directions within the same object. Within the hermeneutic approach of mediation, Don Ihde calls the possibility for multiple interpretations of a technology "multistability"(Ihde 2009, 12-15). Multistability however is indifferent to intentions. Moral appropriation focusses on emerging uses and practices that were not intended by designers. Different intentions do not necessarily have

to be framed in terms of a power dialectic. However, when forms of resistance are present they will become visible in the form of opposite ways of moral appropriation.

With this model a theory can be build in which privacy is defined as material. Whilst (the technology of) privacy has been extensively researched from an ethical perspective (DeCew 1997), a legal perspective (Solove 2006; Solove, Rotenberg, and Schwartz 2011) and a social perspective (Nissenbaum 2004; 2009), a material perspective is still lacking. Such an addition to existing theory could be of importance not only to cultural studies, but also society as a whole. Where ethics, policy and laws have failed to protect consumers of communication technologies, a new material theory of privacy could result in valuable insights in the position of privacy and its materiality within society and culture.

7. Conclusion

In this age of Big Data, privacy is mediated by technologies. Privacy in Big Data systems is not only the result of existing social norms, but is actively shaping them. Privacy in terms of contextual integrity as defined by Nissenbaum (2004; 2009) is way of analyzing contemporary privacy issues that goes further than the classical private/public dichotomy by also taking context into account. By looking at norms of appropriateness and norms of distribution a more detailed analysis can be made of the privacy matters at hand. The affordances of Big Data systems can be in conflict with these norms. Especially the relationality and indexicality in combination with a violation of the norms of distribution can become a threat to society. This is the case when personal communications can be linked to specific people and political or ideological groups.

Mediated privacy in WhatsApp is functions as a black box in which privacy has become a metaphor. Several contexts are purposefully left out of the design and third parties are barely mentioned in the privacy statement and user agreement. The encryption WhatsApp advertises is only effective against hackers, but not against WhatsApp itself, and therefore it affords using the system as a means of mass surveillance. The government is likely to appropriate WhatsApp for this very goal, since they have been known to use other ways of digital communications for similar purposes. They even go as far as fighting possible intrusions of this ability.

Telegram on the other hand attempts to be transparent. They share their code and in the company communications as well as in their design, privacy has an important and very visible role. They purposely choose to make privacy an option instead of a default value to prevent becoming a black box themselves. Quite ironically they need new black boxes, such as the encryption visualization (see cover) to make parts of their system visible to the user. However, with their efforts they are able to do more than just resist. They are effectively shaping privacy in a different way than most popular contemporary applications, such as WhatsApp, Facebook and Google.

For the analysis of privacy applications now in the future, a material definition of privacy could be very valuable. Such a material definition will be able to make visible the metaphoricity and hidden affordances of contemporary communication technologies. Because this material theory is based on moral affordance, moral design and moral appropriation it has room for multiple interpretations and is therefore able to go beyond a dialectical interpretation of the morality of technology. Using the term moral appropriation will open the possibility to discuss multiple instances of moral mediation in one object.

With analysis of both the case studies and the methodology I have shown that contemporary digital communication technologies translate morality in a very specific way. The theory of moral mediation is valuable but falls short when it has to deal with multiple interpretations. A triad of moral affordance, moral design and moral appropriation could offer new possibilities for the analysis of the materiality of privacy and propel ongoing discussions concerning privacy in today's society.

Possibilities for further research go beyond the analysis of other contemporary communication technologies with the same model. Because of the hermeneutic approach to the mediation of privacy in the objects, less attention was given to praxis. However, the analysis has shown that some of the affordances of Telegram in particular invite the user to take part in the process, making privacy a practical matter. This could be further investigated with a practical approach to mediation. Another limitation of the chosen approach in the analysis is the limited visibility of the power structures in place. However, as discussed previously, this problem can be countered by investigating multiple ways of moral appropriation of a technology. Furthermore, the constructed moral triad offers possibilities

to investigate the mediation of privacy from a media archaeological point of view. With such research it could be made visible how privacy changed from being mediated by physical and mechanical technologies to being mediated digitally.

It should be noted that a material understanding of privacy could result in privacy becoming a commodity. It would therefore run the risk of becoming exclusively available for people and entities that can afford it. A material approach to privacy should be seen as a valuable addition and not as a replacement of existing theory, law and practice. To conclude and summarize on a more popular and positive note, emphasizing importance and materialit: Privacy is a thing now.

Bibliography

For purposes of clarity I have split the bibliography in primary (popular) and secondary (academic) sources.

Primary sources

Barlow, J. P. "Declaration of Independence for Cyberspace." https://projects.eff.org., accessed June 11, 2013, https://projects.eff.org/~barlow/Declaration-Final.html.

BBC News. "Telegram Offers Award to Crack Encryption." BBC News, last modified December 19, 2013, accessed March 15, 2015, http://www.bbc.com/news/technology-25444035.

Dredge, Stuart. 2014. "Worried about Leaky Chats? Messaging Apps are Responding with Security Features." *The Guardian*, December 11, np.

Edwards, Jim. "The iPhone had Better be Amazing and Cheap, because Apple is Losing the War to Android." Business Insider, last modified May 15, 2014, accessed March 15, 2015, 2015, http://www.businessinsider.com/iphone-v-android-market-share-2014-5?IR=T.

Electronic Frontier Foundation. "Secure Messaging Scorecard.", last modified March 6, accessed March 8, 2015, https://www.eff.org/secure-messaging-scorecard.

Greenberg, Andy. 2014. "Whatsapp just Switched on End-to-End Encryption for Hundreds of Millions of Users." *Wired*, November 18.

Greenwald, Glenn. 2014. *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State*. London: Penguin Books.

Griffin, Andrew. "Whatsapp and iMessage could be Banned Under New Surveillance Plans." The Independent, last modified January 15, accessed March 5, 2015, http://www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-and-snapchat-could-be-banned-under-new-surveillance-plans-9973035.html.

Jackson, Eric. "Why Selling WhatsApp to Facebook would be the Biggest Mistake of Jan Koum's and Brian Acton's Lives." Forbes, last modified February 20, 2014, accessed March 15, 2015, http://www.forbes.com/sites/ericjackson/2012/12/03/why-selling-whatsapp-to-facebook-would-be-the-biggest-mistake-of-jan-koums-and-brian-actons-lives/.

Jaffe, Gregg and Zezima, Katie. "Obama, Cameron to Discuss Encryption of Online Services." The Washington Post, last modified January 15, accessed March 5, 2015, http://www.washingtonpost.com/politics/obama-cameron-to-discuss-encryption-of-online-services/2015/01/15/e215effe-9ceb-11e4-96cc-e858eba91ced_story.html.

Olson, Parmy. "Whatsapp Hits 600 Million Users, Founder Says." Forbes, last modified August 25, accessed March 5, 2015, http://www.forbes.com/sites/parmyolson/2014/08/25/whatsapp-hits-600-million-active-users-founder-says/.

Open Whisper Systems. "Open Whisper Systems Partners Up with Whatsapp to Provide End-to-End Encryption.", accessed Februari 25, 2015, https://whispersystems.org/blog/whatsapp/.

Oremus, Will. "Obama Wants Tech Companies to Install Backdoors for Government Spying." Slate, last modified January 19, accessed March 5, 2015, http://www.slate.com/blogs/future_tense/2015/01/19/obama_wants_backdoors_in_encrypted_messaging_to_allow_government_spying.html.

Poitras, Laura. 2014. *Citizenfour*. USA: Praxis Films; Participent Media; HBO Films;.

Shu, Catherine. "Meet Telegram, A Secure Messaging App from the Founders of VK, Russias Largest Social Network Site." TechCrunch, last modified October 27, accessed March 15, 2015, http://techcrunch.com/2013/10/27/meet-telegram-a-secure-messaging-app-from-the-founders-of-vk-russias-largest-social-network/.

Snowden, Edward. "We are Edward Snowden, Laura Poitras and Glenn Greenwald from the Oscar-Winning Documentary CITIZENFOUR. AUAA." Reddit, last modified February 24, accessed March 5, 2015, https://www.reddit.com/r/IAmA/comments/2wwdep/we_are_edward_snowden_laura_poitras_and_glenn/.

Telegram. "FAQ for the Technically Inclined.", last modified 2015, accessed March 15, 2015, https://core.telegram.org/techfaq.

———. "Hiding Last seen Time - done Right.", last modified November 19, 2014, accessed March 15, 2015, https://telegram.org/blog/privacy-revolution.

———. "MTProto Mobile Protocol.", last modified 2015, accessed March 15, 2015, https://core.telegram.org/mtproto.

———. "Secret Chats, End-to-End Encryption.", last modified 2015, accessed March 15, 2015, https://core.telegram.org/api/end-to-end.

———. "Source Code.", last modified 2015, accessed March 15, 2015, https://telegram.org/apps#source-code.

———. "Telegram F.A.Q.", last modified 2015, accessed March 15, 2015, https://www.telegram.org/faq#q-how-is-telegram-different-from-whatsapp.

———. "Telegram F.A.Q." Telegram, last modified 2015, accessed March 15, 2015, 2015, https://www.telegram.org/faq.

———. "Winter Contest Ends.", last modified March 2, 2014, accessed March 15, 2015, https://telegram.org/blog/winter-contest-ends.

Tsotsis, Alexia. "Telegram Saw 8M Downloads After WhatsApp Got Acquired." TechCrunch, last modified February 24, accessed March 15, 2015, http://techcrunch.com/2014/02/24/telegram-saw-8m-downloads-after-whatsapp-got-acquired/.

WhatsApp. "About WhatsApp.", last modified 2015, accessed March 15, 2015, http://www.whatsapp.com/about/.

———. "Terms of Service.", last modified July 7, accessed March 15, 2015, http://www.whatsapp.com/legal/#Privacy.

———. "WhatsApp Open Source.", last modified 2015, accessed March 15, 2015, https://www.whatsapp.com/opensource/.

———. "Why we Don'T Sell Add'S.", last modified 2015, accessed March 15, 2015, http://blog.whatsapp.com/245/Why-we-dont-sell-ads.

WhatsApp Support Team. "Frequently Asked Questions - are My Messages Secure?", last modified 2015, accessed March 15, 2015, https://www.whatsapp.com/faq/en/general/21864047.

Zuckerberg, Mark. "Mark Zuckerberg's Full Statement on Facebook Buying WhatsApp." The Guardian, last modified February 20, 2014, accessed March 15, 2015, http://www.theguardian.com/technology/2014/feb/20/mark-zuckerberg-statement-facebook-buying-whatsapp.

Secondary sources

Borgmann, Albert. 1992. "The Moral Significance of the Material Culture." *Inquiry* 35 (3-4): 291-300.

boyd, danah and Kate Crawford. 2012. "Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon." *Information, Communication & Society* 15 (5): 662-679.

Chemero, Anthony. 2003. "An Outline of a Theory of Affordances." *Ecological Psychology* 15 (2): 181-195.

Feenberg, Andrew. 1992. "Subversive Rationalization: Technology, Power, and Democracy 1." *Inquiry* 35 (3-4): 301-322.

Gibson, James J. 1979. *The Ecological Approach to Visual Perception*. Boston: Houghton Mifflin.

Hutchby, Ian. 2001. "Technologies, Texts and Affordances." *Sociology* 35 (2): 441-456.

Ihde, Don. 2009. *Postphenomenology and Technoscience: The Peking University Lectures*. SUNY Series in the Philosophy of Social Sciences. Albany, NY: State University of New York Press.

———. 1990. *Technology and the Lifeworld: From Garden to Earth*. Bloomington: Indiana University Press.

Kitchin, Rob. 2014a. "Big Data, New Epistemologies and Paradigm Shifts." *Big Data & Society* 1 (1): 1-12.

———. 2014b. *The Data Revolution: Big Data, Open Data, Data Infrastructures and their Consequences*. London: Sage.

Laney, Doug. 2001. "3D Data Management: Controlling Data Volume, Velocity and Variety." *META Group Research Note* 6.

Latour, Bruno. 1991. "Technology is Society made Durable." In *A Sociology of Monsters: Essays on Power, Technology and Domination*, edited by John Law, 103-132. London: Routledge.

Lehmann, Ann-Sophie. 2012. "Taking the Lid Off the Utah Teapot Towards a Material Analysis of Computer Graphics." *Zeitschrift Für Medien-Und Kulturforschung* 2012 (1): 169-184.

Leonardi, Paul M. 2010. "Digital Materiality? how Artifacts without Matter, Matter." *First Monday* 15 (6).

Manovich, Lev. 2001. *The Language of New Media*. USA: MIT press.

Mayer-Schönberger, Viktor and Kenneth Cukier. 2013. *Big Data: A Revolution that Will Transform how we Live, Work, and Think*. New York, NY: Houghton Mifflin Harcourt Publishing Company.

Montfort, Nick and Ian Bogost. 2009. *Racing the Beam: The Atari Video Computer System*. USA: Mit Press.

Nissenbaum, Helen. 2004. "Privacy as Contextual Integrity." *Washington Law Review* 79: 101-139.

———. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.

Norman, Donald A. 1999. "Affordance, Conventions, and Design." *Interactions* 6 (3): 38-43.

Regan, Priscilla M. 1995. *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill: University of North Carolina Press.

Sawicki, Jana. 2003. "Foucault and Heidegger: Escaping Technological Nihilsm." In *Foucault and Heidegger: Critical Encounters*, edited by A. Milchman and A. Rosenberg, 55-73. Mineapolis: University of Minnesota Press.

Schäfer, Mirko Tobias. 2011. *Bastard Culture!: How User Participation Transforms Cultural Production*. Vol. 6 Amsterdam University Press.

Solove, Daniel J. 2006. "A Taxonomy of Privacy." *University of Pennsylvania Law Review* 154 (3): 477-564.

Turner, Fred. 1999. "Cyberspace as the New Frontier?: Mapping the Shifting Boundaries of the Network Society." *Red Rock Eater News Service*: April 1, 2015.

van den Boomen, M. V. T. 2014. "Transcoding the Digital: How Metaphors Matter in New Media." *Theory on Demand* 14.

Verbeek, Peter-Paul. 2006a. "Materializing Morality Design Ethics and Technological Mediation." *Science, Technology & Human Values* 31 (3): 361-380.

———. 2006b. "Materializing Morality: Design Ethics and Technological Mediation." *Science, Technology & Human Values* 31 (3): 361-380.

———. 2011. *Moralizing Technology: Understanding and Designing the Morality of Things*. Chicago: University of Chicago Press.

———. 2014. *Op De Vleugels Van Icarus: Hoe Techniek En Moraal Met Elkaar Meebewegen*. Rotterdam: Lemniscaat.

———. 2013. "Resistance is Futile." *Techne: Research in Philosophy and Technology* 17 (1): 72-92.

———. 2007. "The Technological Mediation of Morality - A Post-Phenomenological Approach to Moral Subjectivity and Moral Objectivity." In *Philosophy and Design: From Engineering to Architecture*, edited by P. E. Vermaas, P. Kroes, A. Light and S. Moore, 91-103. Dordrecht: Springer.

Walzer, Michael. 1983. *Spheres of Justice: A Defense of Pluralism and Equality*. New York: Basic Books.

Winner, Langdon. 1986. "Do Artifacts have Politics?" In *The Whale and the Reactor: A Search for Limits in an Age of High Technology*, edited by Langdon Winner, 19-39. Chicago: University of Chicago Press.

Wittgenstein, Ludwig. 1958. *Philosophical Investigations*. Translated by G. E. M. Anscombe. Oxford: Basil Blackwell.

Zikopoulos, Paul, Chris Eaton, Dirk Deroos, Tom Deutsch, and George Lapis. 2012. *Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming Data*. New York, NY: McGraw-Hill.