In Technology We Trust:

Cloud Computing, Technical Breakdowns and the Protection of Privacy

by

Brian Clarke

A thesis submitted to the Faculty of Graduate and Postdoctoral Affairs

in partial fulfillment of the requirements for the degree of

Master

in

Sociology

Carleton University

Ottawa, Ontario

Abstract

This thesis looks at the 'trade-off' that users of cloud computing services must make: convenience of use in exchange for outsourcing the protection of private data. In particular, it looks at the relationship of trust that must exist in this exchange. Using concepts from actor-network theory, I explore how this trust in a technological entity is formed, maintained and broken. Using Dropbox as a case study, I analyze the relationship between a cloud computing service and its users by performing a textual analysis of privacy policies and other official communications, as well as threads on user help forums. I find that the cloud computing provider (Dropbox) works to establish its reliability and trustworthiness and it is only in instances of breakdown – when this reliability is questioned – that the privacy 'trade-off' and issues of protecting personal data become contested.

Acknowledgements

First and foremost, I would like to thank Dr. Carlos Novas for his continued guidance, and patience, as well as his immense knowledge provided while supervising this thesis. I would also like to express gratitude to my other committee members, Dr. Michael Mopas and Dawn Moore.

I would also like to express thanks to my many peers and colleagues, particularly Derek Silva, Justin Tetrault, Alex Castleton, Rhys Williams and Ben Todd, who through many discussions and debates have helped my thinking abilities to grow over the past two years.

And last but not least, I'd like to thank my wife, Simona Maliszewska, for her ongoing patience and encouragement, and for not allowing the stresses of graduate work to overwhelm me.

Table of Contents

List of Appendices

1 Introduction

In 2010, the Office of the Privacy Commissioner (OPC) of Canada (2011) held consultations and published a report regarding the risks, benefits and governance of cloud computing. The OPC concluded that while there are certainly benefits to using cloud computing, particularly for organizations; however they also present a number of privacy risks that are often misunderstood and underestimated. In particular, privacy protection and the handling of personal data are outsourced to a third party, often in another jurisdiction. The OPC summarizes these issues:

> "When it comes to cloud computing, the security and privacy of personal information is extremely important. Given that personal information is being turned over to another organization, often in another country, it is vital to ensure that the information is safe and that only the people who need to access it are able to do so. There is the risk that personal information sent to a cloud provider might be kept indefinitely or used for other purposes. Such information could also be accessed by government agencies, domestic or foreign (if the cloud provider retains the information outside of Canada)" (Office of the Privacy Commissioner of Canada 2011).

In other words, if data availability or data confidentiality are compromised "customers could incur substantial losses" to their privacy and personal information, which could include financial information, intellectual privacy, or personal or organizational secrets (Das, Classen, and Davé 2013: 21).

These consultations led to increased research and reporting from the OPC on cloud computing and the changing landscape of data privacy, and likely influenced the recommended changes to Personal Information Protection and Electronic Documents Act (PIPEDA) brought before Parliament in 2013. If we follow the simple assumptions of Bijker and Law (1992: 3) that all technologies involve social relations and that "always

embody compromise" then in the case of cloud computing, this compromise involves a 'trade-off' of the use of cloud computing services in exchange for personal data and privacy risks. This trade-off is often explicitly laid out in two important documents that most cloud computing services provide to their users: the terms of agreement and privacy policy (Bodle 2011). These documents represent the contract between the service provider and users, who agree to give up some rights to their personal data in order to use the service. However, as I will discuss in Chapter Two, several scholars have highlighted issues with these contracts, arguing that they do not function well as a contract between two equal parties.

Using Dropbox as a case study of a cloud computing service, the thesis seeks to understand the nature of this trade-off of use for privacy risks. I propose to incorporate actor-network theory to look at how this trade-off can be understood as a negotiation between a technology and its users. In doing so, I look at trust as a particularly important mechanism in this trade-off. In other words, rather than understanding this trade-off as an exchange in which privacy is the currency, I seek to explore the role trust plays and how privacy itself is fragmented, contextual and negotiable in this interaction between technology and users. I ask how Dropbox prescribes a particular set of privacy values to users and how these users might interpret, accept, negotiate or resist these scripts.

What is cloud computing?

First, I will provide a brief review of what cloud computing is and further explain why privacy is an issue. Cloud computing is defined by the United States National Institute of Standards and Technology (NIST) as:

> "A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage,

> applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." (National Institute of Standards and Technology 2011)

In a similar vein, Mather, Kumaraswamy and Latif (2009) add that there are five common attributes of all cloud computing services: shared resources, massive scalability, elasticity, pay as you go and the self-provisioning of resources. While these definitions are technical and bureaucratic, they do provide some starting points to discuss what cloud computing is and how it can be analyzed sociologically. In simpler terms, cloud computing broadly refers to computing services, software and platforms that are not owned individually by users and installed locally on their personal computer, but rather accessed via an Internet connection. For example, common cloud-based applications include cloud storage services, such as this project's case study: Dropbox. These services allow users to store files on an external, shared server rather than on their own hard drives. These types of services highlight the benefits and risks of cloud computing: they give users access to online storage space that can be accessed conveniently from any computing device, but also delegates the responsibility of protecting one's privacy and securing one's data to an unknown third party.

An important idea regarding cloud computing is that it is not a static entity, but rather a fluid, broad and overarching concept. Cloud computing is not necessarily a new technology, but rather a new idea. It is not one technological artefact but is rather the result of several technological improvements (Mather, Kumaraswamy, and Latif 2009). It is not a homogenous technology but rather a heterogeneous network of technologies, corporations, users and governments that has allowed this new thing – cloud computing – to emerge. Additionally, there are many different uses for cloud computing services,

ranging from simple web email clients and online file storage services to whole operating systems offered through an Internet connection. For these reasons, once again following the actor-network approach outlined by Bruno Latour, John Law and others (Latour 1992; Law 1991), I want to avoid thinking about cloud computing as a technology or as a single artefact, but rather think of it as an assemblage that is composed of many heterogeneous elements: computing hardware and software, social and political actors, and discourses and ideas. These heterogeneous actors and associations that comprise 'cloud computing' may be more or less stabilized. One goal of this project is to explore the relative stability of this assemblage. Instead of seeing privacy as an inherent social value that is being exchanged for use of the cloud computing service, this project works from the assumption that privacy values are multiple and contextual. Can we understand cloud computing as a stable network in which users must adhere to standard practices and understandings of privacy? Or is this cloud computing network one in which user subjectivities are multiple, contested and negotiated?

From these characteristics of cloud computing, two ideas are of sociological significance. First, the idea of "convenient, on-demand" (National Institute of Standards and Technology 2011) services fits into the idea of what some authors have called a 'convenience culture.' For example, Tierney (1993) argues that one of the defining features of modernity is the consumption of 'conveniences.' He defines convenience as an "ability to mitigate the effects of bodily limits"; for something to be convenient it must make easy and simple an action that was previously difficult, impossible or troublesome (Tierney 1993: 38-39). Modern subjects, argues Tierney (1993: 6), consume new

technologies in a way that satisfies a desire for ease which leads to the development of a technological culture or what he calls "technological fetishism."

The advances and development of cloud computing are certainly compatible with this argument; the benefits of consumption or use of cloud computing relate to this value of convenience. Something that was previously limited – file and data storage and access across multiple platforms – now becomes easy and simple. Users are able to easily, quickly and conveniently access computing services across multiple times, locations and devices, rather than being limited to one personal computer. Tierney (1993) argues that for an object to be convenient it must be suitable with the self or the subject. It must be comfortable and readily usable for the user in his or her daily life. The benefits and marketing of cloud computing services are often framed in similar language: modern individuals are meant to be always connected to the Internet, to their work and to their social networks across multiple computing devices and cloud computing suits this lifestyle by synchronizing these devices. In other words, cloud computing can be understood as a technological development within this culture of convenience.

Second, the idea of "shared pool of… resources" (National Institute of Standards and Technology 2011) highlights the social aspect of cloud computing. While I am starting from the assumption of the actor-network school of thought that all technology is inherently social (Bijker and Law 1992; Latour 1991; Latour 1992), cloud computing services particularly highlight the importance of sociological analysis of a new technology. As the above definition and characteristics of cloud computing show, cloud computing is never used in isolation. Since users are using the technology through an Internet connection, they are always using the technology in connection with other actors:

most notably the corporation running the service, but also indirectly other users. In other words, because cloud computing represents a 'shared pool of resources,' users are never completely isolated from important social relations.

A final, important distinction to make is that between private and public clouds. Public clouds (Mather, Kumaraswamy, and Latif 2009) are defined as cloud services available to anyone (e.g.: webmail), as compared to private clouds that are only available to users within the organization that owns the technology (ex: an internal corporate email system) (Office of the Privacy Commissioner of Canada 2011). As Mather and his colleagues show (2009), most small organizations do not have the resources to implement a private cloud and therefore use public cloud services, sacrificing some security benefits for affordable services. Additionally, the boundaries of public clouds are by definition much more open and fluid, potentially giving rise to more interesting associations and negotiations. For these reasons, throughout this thesis I will mostly be discussing public cloud computing networks, unless otherwise noted.

Why is privacy an issue with cloud computing?

Although the benefits of cloud computing are widely discussed in popular culture and the media, several commentators have raised concerns regarding data privacy and security in the cloud. As shown above, Canada's Office of the Privacy Commissioner has made the issue one of utmost importance in the future of data privacy, by publishing a series of resources for users and organizations to protect their privacy while using cloud computing technologies. As argued by Robert Bodle (2011), there is an implicit exchange happening with the use of cloud computing: users 'pay' for the use of the technology by giving up ownership of certain personal data. In other words, private data

becomes a commodity (Andrejevic 2007). However, why is third party ownership of private data problematic? In short, this data is almost always used for secondary purposes, typically targeted advertising (Andrejevic 2007; Bodle 2011), but can also be used for political surveillance (Fuchs, Boersma, Albrechtslund, and Sandoval 2012).

In exploring the privacy concerns of various members during their consultations, the OPC (2011) came up with two reasons why third party ownership of personal data could be problematic: jurisdiction and third-party access. They state that "cloud computing is largely borderless," (Office of the Privacy Commissioner of Canada 2011) meaning that often users are accessing data stored in other jurisdictions. As Jaeger et al. (2009) show, data centers that store users' data are typically built in jurisdictions with ideal conditions – lots of land, abundant energy and natural resources, and most importantly, favourable corporate law and taxes. Thus, on the one hand, ownership of personal data is blurred between users and cloud service providers while on the other hand, the rules governing this exchange, ownership and use of personal data is even more obscure. As both the OPC (2011b) and Jaeger et al. (2009) point out, the global nature of cloud computing makes it difficult to govern.

The problem of third-party access refers to the concern of cloud computing users that parties other than the service provider with whom they have entered into an agreement, can access their data (Office of the Privacy Commissioner of Canada 2011). Providing personal data solely to the cloud service provider without any third party access is problematic on its own; Bodle (2011) shows how Google, the largest provider of cloud services, has vague privacy policies and terms of agreement that give rise to several issues such as unclear user rights and responsibilities and an unclear account of

how Google will employ its users' personal data. However, third party access further confounds the issues of who owns the data and what they can (or will) do with it. As the OPC (2011b) shows, users are particularly uneasy about access by foreign governments: "concerns were expressed about the risks of outsourcing personal data for processing in countries with laws that allow arguably easier access to the data on the part of governments than do the laws in Canada."

This matter is further complicated when the user of the cloud computing technology is not the owner of the data being provided. In their consultations regarding cloud computing and privacy, the OPC (2011b) makes the important distinction between data processors and data collectors. When an individual is using a cloud service, such as a webmail application, the service provider is both the processor and the collector. However, when an organization collects data from a client or participant and stores it using a cloud computing network, the division between a data collector and processor becomes unclear. In these situations, the issue of who has what rights and responsibilities regarding the personal data becomes increasingly complex. This raises concerns in several potential practices of cloud computing, such as academics using cloud services to store research notes or lawyers using cloud-based invoicing software; in both these examples, the data collector is bound by rules of confidentiality with the owner of the data, raising additional privacy concerns when a third-party data processor is involved.

A final problem regarding third-party access comes from unsolicited access to personal data (Mather, Kumaraswamy, and Latif 2009), particularly from hackers. This is particularly problematic with public clouds. As discussed above, many individuals and small organizations will opt to use public cloud computing services, sacrificing security

for affordable uses. The downside to these public clouds is that they are more prone to attacks from hackers than a private cloud. Additionally, when complex situations discussed above arise with different persons, data collectors, data processors and potentially other third-parties in other jurisdictions, the potential harm from a public cloud computing network is amplified.

Structure of this Thesis

My central argument in this thesis is that one must look at *trust* as a central concept in order to understand the trade-off in which privacy risks are exchanged for use of cloud computing services, in a way that grants agency to both parties of this exchange. Another way of framing this 'trade-off' of which I have discussed above is that customers are required to place a certain level of trust in the cloud computing services they wish to use. This thesis delves into this relationship of trust. How can users trust a distant entity 'in the cloud'? How can this trust be understood sociologically? And what implications does this have for debates on data privacy and privacy protection?

Trust is an interesting concept that arises in varying ways in sociological thought. Sztompka (1999: 25) broadly defines trust as "a bet about the future contingent actions of others." Trust involves a dependency on other social actors in order for social order and the predictability of action. This conceptualization of trust is crucial in functionalist and social systems thinking. For instance, Durkheim's (1933 [1983]) classical concept of organic solidarity essentially boils down to trust: in a society in which a highly differentiated division of labour exists, what holds people together is mutual dependency, or the trust that one can rely on another for a function that they cannot provide themselves. Moreover, Luhmann (1979 [1973, 1975]) argues that trust is a medium of

communication that is required in modernity. For Luhmann (1979 [1973, 1975]), modern society has become functionally differentiated into self-reproducing subsystems (i.e., politics, law, economy); trust is but one medium of communication for these subsystems of society that serve to reduce the complexity that has resulted from this functional differentiation. Giddens (1990) expands on this Luhmannian view and argues that a defining feature of late modernity is the need for trust in order to reduce complexity and uncertainty, and to be able to have a sense of control and to predict social action. While the nuances of these various understandings of trust are different, the common theme for understanding trust is the relationship between differentiation and trust. As action becomes differentiated, trust in other actors is needed. Heterogeneity necessitates trust.

Sztompka (1999) argues that trust is a human trait; we do not put our trust in natural actions such as weather-related or geographical happenings. I would disagree. If trust is understood as in terms of differentiation and predictability, we can certainly place trust in certain meteorological phenomenon, such as seasonal change, in order to base action. This trust in non-humans is particularly noticeable in technology. We trust technological artefacts and programmes to behave as expected. This phenomenon will become clear as I discuss cloud computing and black boxed technologies. Since technologies involve differentiated action amongst heterogeneous and mutually dependent actors, there must be some trust between these actors. This understanding of trust and technology serves as the basis for my argument that trust should be a central conceptual concern when discussing cloud computing and privacy.

I will advance this argument as follows. In Chapter Two, I discuss various approaches to understanding cloud computing and data privacy. Since literature on cloud

computing is scarce, I focus on understanding how data privacy has been conceptualized in the academic literature. I outline three schools of thought on data privacy: business literature, which tends to see privacy as an appropriate sacrifice for new efficient information technologies; communication, legal, and policy literature that places emphasis on the nature of privacy, how it changes with the introduction of new communication technologies, and how such changes are to be regulated; and surveillance studies that focus on the rationales and logic behind data collection. While each of these schools of thought adds some important insight into the relationship between new technologies and data privacy, I argue that they all tend to treat users as passive; technology is the main actor in all of these views as it either transforms or represses individual privacy. They do not question what users see or understand as private, privacy, or privacy protection. While this thesis does not necessarily fill this gap, it is an attempt to think about how user agency can be articulated in the trade-off between users and cloud computing service providers. The concept of trust, I argue, provides a useful starting point; users actively entrust entities (technological or otherwise) external to themselves.

In Chapter Three, I outline my theoretical framework for looking at users, agency and the trade-off involved in cloud computing services. I argue that actor-network theory is a useful tool for these purposes, for several reasons. First, one of its central tenets is to be symmetrical and grant equal agency to all actants. The concepts of script and de-scription (Akrich 1992) are particularly important, as they involve an explicit attempt to understand the relationship between users and technologies, while assuming both can act. Second, the metaphor of the black box, used commonly in actor-network theory, provides

a useful conceptual framework for understanding trust, delegated action and the user-technology relationship. In this chapter, however, I also consider some critique of actor-network theory, particularly that of Star (1991) on the 'executive approach' of this school of thought. I argue that incorporating Star's (1991) critique is beneficial to my project as it plays close attention to individual difference, marginality and the ability to act in human users.

In Chapters Four and Five, I begin tackling the questions of trust and privacy through a case study of Dropbox. In Chapter Four, I look at Dropbox's official communications (policies and company blog posts) to explore what kinds of user scripts it prescribes to its users; what sorts of competencies, behaviours and actions are expected of users? What does Dropbox assign to itself? Three findings were observed. First, Dropbox expends much effort on communicating its trustworthiness. Users are expected to trust Dropbox as an objective technical object with a high level of technical expertise. Second, Dropbox makes clear that data security is its responsibility. This serves to further the trustworthiness of Dropbox. Lastly, privacy protection is expected to be the responsibility of users. While Dropbox and its security are designated as objective, durable and trustworthy, users are portrayed as subjective and prone to error and thus expected to maintain a constant vigilance when regulating one's own privacy.

In Chapter Five, I turn to users themselves to see how they interact with and respond to these user scripts through an examination of Dropbox's user help forums. I find that most users act in conformity with Dropbox's expected and ideal user, signalling some level of stability in the technology and standardization of use. However, keeping in mind Star's (1991) critique of actor-network theory and the importance of individual

difference, I also explore the multiplicity and marginality of users. Users have varying levels of trust in Dropbox. However, other users typically attempt to rearticulate Dropbox's trustworthiness and reliability. This presents an interesting tension between these marginal users hanging on to their marginality and the efforts of Dropbox and its enrolled users to reduce this marginality and further standardize the use of the technology. Lastly, I look at particular instances of breakdown – when Dropbox does not behave as expected. It is in these situations, I conclude, that trust is breached and the clear delegation of duties and responsibilities regarding privacy become contested. In other words, the trade-off users experience in order to use the cloud computing service becomes negotiable when the central tenet of this trade-off – trust – becomes muddled.

Lastly, in Chapter Six, I explore the implications of this conclusion. First, I draw out some of the theoretical implications of my analysis, namely the connection between trust and technologies. I argue that technologies that have been black-boxed, that have become so stable and taken-for-granted that their internal parts cease to be questioned, require some level of trust on a general level. Trust is not only an important concept when speaking of cloud computing but is also important when talking about technology and objectivity more generally. Next, I draw out some practical implications of this study for users of cloud computing. My goal here is to introduce just a bit of mistrust into the use of these services: not so much distrust that these services cannot be used, but rather just enough that cloud computing is not treated as a black-boxed technology and its components can still be observed and questioned. This can allow users to have greater choice in deciding if individual actors can be trusted with the delegated responsibilities of protecting personal data. And finally, I lay the groundwork for how this discussion of

trust can be worked into policy debates, such as those in which the OPC is involved. I argue that accountability is an important criterion for trust and thus to conclude, I endorse further policy debates that focus on the accountability of parties collecting personal data rather than debates that focus solely on technical safeguards for privacy protection.

2 Approaches to Understanding Cloud Computing and Data Privacy

This chapter will outline various theoretical and empirical approaches scholars have taken to understand cloud computing and data privacy more generally. Since the literature on cloud computing is limited – due to the relative youth of the technology – the scope of the literature I will review touches on larger questions about data privacy and privacy on the Internet. My goal is not to provide a comprehensive review of the literature on privacy and the Internet but rather to outline different approaches that have been taken. I will outline three empirical traditions that can be identified in the literature. For each of these approaches, I will highlight some of the main ideas and explore the strengths and weaknesses of applying them to cloud computing and data privacy. First, I will discuss the business and communications literature that largely focuses on the benefits of cloud computing but ignores the question of privacy. Second, I will discuss critical communication and legal studies that seek to fully develop the concept of privacy and its philosophical and juridical connotations. Third, I will discuss surveillance literature that places data privacy into questions of surveillance and security. Throughout this chapter, I will make the argument that a common drawback of these various approaches is that they treat users as passive actors. As a potential alternative that respects the active agency of users, I conclude by exploring some recent literature that looks at the nexus of trust and privacy as a potential alternative.

Business & Communication Literature: Convenience & Economic Growth

Most of the business literature and business-oriented communications research focuses solely on the benefits of cloud computing and treats privacy as an afterthought, if at all. Thus, I will not review this literature in too much detail as it does not relate to my

project of exploring users' data privacy. Nevertheless, it is still important to briefly introduce this popular, futurist point of view as it explains why users employ cloud computing, despite privacy risks. In other words, it outlines one side of the compromise or trade-off that Bijker and Law (1992) argue is inherent in all technology. In the case of cloud computing, its apparent benefits are convenience and ease of access. Often this argument for convenience is advanced using an economic discourse, particularly for use of cloud computing by organizations: by freeing workers from the limits of traditional computing models, multiple users can access the same project from multiple locations which saves time, increases efficiency and productivity, and ultimately increases profits[1]. In other words, cloud computing is consistent with what Sennett (1998) calls "flexible capitalism," referring to the modern work landscape in which employees are expected to be flexible, mobile and efficient, which is contrasted with traditional Taylorism in which workers are compartmentalized.

One of the leading works in this economic-communication approach is Benkler's *The Wealth of Networks* (2006). While he does not directly address cloud computing, Benkler makes an economic argument for Web 2.0, social networking and collaborative work tools which has a clear carry over to cloud computing technologies. Like Sennett (1998) who argues we are entering a new form of capitalism, Benkler (2006) argues that a new information economy is emerging. He argues that the new economy, as opposed to the twentieth century mass society, is based on decentralization, peer production and sharing. The stimulus for this shift is cheaper and more widespread access to computing

[1] For example, Jones (2012) discusses how organizations can efficiently manage personal information 'in the cloud', while Mather, Kumaraswamy and Latif (2009) provide organization advice for managing a secure cloud computing framework. Business magazines, popular books and the 'blogosphere' are saturated with similar advice for both large and small businesses. What holds these organizational tips together is the implicit goal of efficiency and profitability.

technologies (Benkler 2006). Thus, Benkler would argue that cloud computing technologies are beneficial from an economic point of view, as they provide further cheap access to computing technologies, particularly for small organizations, which further promotes an economy based on decentralization and peer production.

Another way of advancing this pro-sharing and pro-cloud computing argument using an economic discourse is advanced by Nicholas Carr (2008). Like Benkler, Carr (2008) argues that modern computer technologies, specifically cloud computing, mark a distinct shift in economic history. He compares the shift from traditional computing models to cloud computing models to the rise of electricity in the industrial era. Before cloud computing, users and organizations had to provide their own computing power, similar to before electrification, households and organizations provided their own power. Similarly to how electrification allowed for households to "plug in" to a wider electrical grid, cloud computing now allows users to plug into a computing grid (Carr 2008). Similar to Benkler, he argues this promotes economic growth, as more individuals and organizations are able to access high powered computing services without investing much time or resources (Carr 2008).

Carr (2008) realizes the dangers that this metaphor highlights: that the provision of computing services is monopolized. In other words, modern data centers (the physical location of the cloud computing hardware) are akin to the power plant during the rise of electricity. Thus, unlike Benkler (2006) who argues that new computing technologies promote decentralization, Carr (2008) shows the opposite: cloud computing allows for the centralization of computing services. Despite this acknowledgement, however, Carr (2008) does not explore the consequences of this monopolization. This is the first

weakness of using these business and economic-oriented communication studies for understanding cloud computing. As Jaegar, Grimes, Lin and Simmons (2009) argue, the centralization of computing services into large data centers raises several related issues, such as energy and environmental impact and questions of regulation and jurisdiction.

A larger issue with this approach to studying cloud computing, however, is that little to no discussion is given regarding the privacy implications of these technologies. The discussion of privacy from Benkler (2006) is limited to a short argument that private (as in free from political influence) communication over the Internet is able to now have a wider reach and hence, a greater political effect. However, this argument is very problematic, which will be clear when I discuss the surveillance literature – these empirical projects have made it clear that communication over the Internet is not independent from political structures and relations of power[2]. However, to conclude this section, it is important to stress that the research justifying cloud computing and explaining its economic benefits only explains one side of the equation. If we follow Bijker and Law (1992) and assume that all technologies have an inherent trade-off, it is important to discuss both sides of this trade-off in relation to cloud computing.

Critical Communication and Legal Studies: Theories of Privacy and Practical Solutions

The majority of literature on data privacy comes from the field of communications studies. In this section, I have also grouped legal and policy literature due to similar themes that are addressed in these streams. This literature provides an in-depth exploration of the philosophical and legal meanings of privacy as well as attempts

[2] Christian Fuchs and his colleagues (2012) provide several examples in which online data is used for political surveillance, arguing that the online information economy is ultimately tied up with the broader political economy.

to think about how privacy is to be protected through technical, legal or governmental means. The tradition in communication studies to take a critical look at data privacy stretches far back beyond the rise of cloud computing, with some scholars discussing the topic in the early days of the Internet in the early 1990s. In this section, I will provide a brief review of some of the main communications scholars that have discussed data privacy over the last 20 years, some legal and policy scholars that have used these ideas and proposed legislative solutions, and finally, the few scholars that have used these ideas to discuss cloud computing more recently.

One of the benefits of the communications literature on data privacy is that they have adapted and repurposed some legal and philosophical theories of privacy and applied them to the realm of computing, networks and information and communication technologies (ICTs). As advanced by Tavani (2008), there are generally two ways to conceptualize privacy: rights-based and interests-based privacy. Rights-based views of privacy (Thomson 1975) view privacy as an inherent human right, similar to the right to property or security (Tavani 2008). However, as DeCew (1997: 21) shows, this view is fading in favour of an interest-based conception of privacy, due to the fact that there is no Constitutional right to privacy in the United States[3]: "in many of the more recent privacy cases there has been a shift away from reasoning that takes a rights-oriented approach toward more arguments that use a utilitarian cost-benefits analysis, which balances the costs of privacy and the benefits to public safety and crime control." In other words,

[3] While DeCew (1997) was writing in an American context, the Canadian Charter of Rights and Freedoms (1982) is also absent of any constitutional right to privacy. This is contrasted to the Charter of Fundamental Rights of the European Union (2000), Article 7: "Everyone has the right to respect for his or her private and family life, home and communications".

privacy is not a protected right, but rather there exists an expectation of privacy that is assessed contextually.

Tavani (2008) argues that there are four essential interests that can be included under the rubric of interests-based privacy: physical, mental, decisional and informational. The first is not really applicable in studies of data privacy; physical privacy refers to the interest of non-intrusion of one's physical space. Mental and decisional privacy reflect similar interests: mental privacy refers to the interests of non-intrusion of one's thoughts, while decisional privacy refers to the interest of non-interference with one's ability to make rational choices. While both of these types of privacy can be related to data privacy, and are themes that are clearly picked up in the anti-surveillance literature I will review later, critical communication scholars have largely neglected them and have focused almost exclusively on informational privacy. Informational privacy refers to the interest of controlling and limiting access to one's personal information (Tavani 2008).

A great example of early communications research that discusses data privacy with an overt focus on informational privacy is research advanced by Bennett (1991). Bennett (1991) discusses how policy is underpinned by theoretical and philosophical assumptions, and as such, early policies on data privacy are underpinned by different understandings of the nature of privacy. Comparing data privacy policies in different regulatory regimes, Bennett (1991) concludes that how data privacy is governed varies depending on political and technological traditions. While this is not a novel argument, the key point is that privacy is a historically and spatially variable value. In other words, privacy is a dynamic rather than a static concept (Tavani 2008). Bennett (1991) asks the

important question of whether shifts in this dynamic value are caused by changes in political structures or changes in technologies.

While Bennett (1991) is correct in being cautious about answering this question, the tendency in communications literature and especially the policy/legislative recommendations resulting from this research has leaned towards one of technological determinism. In other words, several authors discussed in this section either explicitly or implicitly take the view that changes in technology have resulted in changes in society and thus necessitate changes in privacy laws. This view is most clearly articulated in an article in the Institute of Electrical and Electronics Engineers' (IEEE) Security and Privacy magazine titled "How internet users' privacy concerns have evolved since 2002" (Anton, Earp, and Young 2010). While the authors of the article concluded that the primary privacy concerns – "information transfer, notice/awareness, and information storage" – have not changed over the eight year study, they do note how users' privacy concerns have been updated to reflect new Internet technologies, such as social networking and cloud computing (Anton et al. 2010). More importantly, the technological determinist assumptions are clear in this study: changes in technologies lead to evolving understandings of privacy.

These determinist assumptions also pervade more scholarly works on data privacy. For example, Smith and his colleagues (2011: 990) argue that "the recent evolution of the concept of privacy in general—and information privacy in particular—follows the evolution of information technology itself." In other words, societal and cultural values follow technological change. A similar idea is presented by Helms (2001), who distinguishes between 'society' and 'technology' and argues that the latter

works on the former in problematic ways. Once again, cultural values of privacy *follow* technological changes; technology is treated as an independent entity that determines changes in society. Helms (2001: 289) states "where society has attempted to protect, technology has attacked," painting the relationship of society and technology as one of conflict, with technology seemingly always one step ahead.

These assumptions can also be noticed in more recent literature on cloud computing. For instance, Couillard (2008) argues that society and law typically lag behind technological changes. This argument is often seen as self-evident or common sense. Cloud computing is but one recent example of this phenomenon: computing advances have created a new privacy landscape and society or humanity must adjust by altering its values, understandings and practices regarding privacy. Couillard (2008) specifically looks at how law should adapt to this evolving landscape.

There certainly is some value in this thinking; much of the motivation for studying technological artifacts is reactionary – how should we react to these new technologies. Nevertheless, the determinist assumptions that technology precedes and determines society or cultural values can be problematic. Boczkowski and Lievrouw (2008) argue communication scholars tend to lean towards this determinist standpoint. While I believe most of the literature above is correct is assuming that new technologies can create new concerns or issues, some of the research has gone further with the determinist assumptions by implying that new technologies cause a change in social relations and user values, perceptions and subjectivities. This assumption can cause problems for sociological research which tends to attach primacy to social relations and look at how society and technology interact with each other (Boczkowski and Lievrouw

2008). Ultimately, the role of human agency is underestimated. The innovative actions of those who invent new technologies[4], the cultural values that allow some technologies to succeed and others to fail[5] and the creative tendencies of users to adapt to or resist technologies in varying ways[6] are left out of the equation. Rather, technological advancements are unquestioned and taken-for-granted. Therefore, instead of assuming that cloud computing causes a change in privacy values and relations, I believe that it is useful to think about how existing values and relations interact with the technology and are involved in 'co-construction of users and technology' (Oudshoorn and Pinch 2003).

Despite these determinist tendencies, communication and legal scholars have proposed several solutions as an attempt for 'society' and users to adapt to cloud computing; most of these solutions are legislative in nature. For example, Tavani (2008) discusses how in the United States new legislation was enacted to deal with one of the most controversial issues of informational privacy: the exchange of medical and health information. While most solutions offered are legislative or policy changes, some scholars have advocated for greater industry self-regulation. As such, most of the proposed regulations and governance of informational privacy involve some sort of governmental or bureaucratic oversight agency (Flaherty 1986).

Nevertheless, all the solutions reviewed in the communication literature falls under one of, or mix of, two theoretical frameworks: restricted access theory and control

[4] The emerging interdisciplinary field of innovation studies explores the conditions of innovation and invention. See the Center for Science & Innovation Studies at University of California, Davis (http://innovation.ucdavis.edu/) for more information.

[5] For instance, Bijker (2007) provides a wonderful comparative analysis of dikes, dams and levees in Amsterdam versus New Orleans, arguing that the political climate influences the development and spread of a given technology.

[6] This is perhaps best studyied by scholars in the field of social construction of technology (SCOT). For example, Kline and Pinch (1996) look at how rural users adapted to the early automobile.

theory (Tavani 2008). The former refers to a view of informational privacy as the ability to restrict access to information about oneself (Bok 1983), and solutions involve setting up "zones" or contexts in which one can effectively limit access to their personal information (e.g., a locked filing cabinet, or laws protecting doctor-patient confidentiality). Control theory, while very similar, advances a slightly different conception of information privacy: one should be able to control information about them. This would include being able to restrict access to others, but if access is granted, one should be able to have the final say on how the information is used (Fried 1990). The central challenge in proposing solutions under control theory is increasing individual choice on how and to whom access to one's information is granted (Tavani 2008).

Whichever theory of privacy protection scholars employ, most take the same object of analysis in proposing solutions: terms of agreement. For instance, restricted access theorists might argue for limiting the amount and types of data that companies can request and require that these limits are reflected in terms of agreement. For example, Jaeger (2013) discusses the development of international standards for what information companies can collect and what they can do with it. While she believes the way this should occur is through industry self-regulation, Kimrey and Clark (2012) argue that it is the responsibility of the legal profession to ensure that personal information is respected. Strong legislation and a strong corporate law profession are needed to restrict access to certain personal information and limit certain privacy risks. The common thread between these two views is that user choice is left out of the discussion; it is implied that users will continue to use the technologies and it is the responsibility of other parties to respect their privacy.

Control theorists, on the other hand, might propose that more detailed information on what personal information will be used for is included in terms of agreement, so that users can make an educated choice about allowing access to their information. Fernback and Papacharissi (2007), for example, provide a good in-depth study of online terms of agreements and privacy policies, and conclude that they offer very little in terms of user control over their data. They suggest that policy changes are needed to govern these online agreements. Furthermore, Samuelson (2000) discusses informational privacy as an intellectual property right, meaning that users should be able to negotiate with firms about the use of their information. However, terms of agreement do not necessarily give room for such negotiation, and are almost exclusively presented in a take-it-or-leave-it fashion (Bodle 2011).

Similarly, Cronin (2000) argues that the primary issue is not that Internet-based technologies pose a threat to personal privacy, but rather that users are left in the dark and confused about how and when their personal information is being used. Echoing the control theory of informational privacy, she argues that users should have more knowledge and choice over the use of their personal information, especially when entering into an agreement or exchange with the Internet company (i.e., when agreeing to terms). Building from this argument in the same volume, Radin (2000) argues that a radical rethinking of contract law is needed to govern online contracts. She argues that online contracts pose a number of problems for traditional contract law, such as unequal bargaining power, unclear jurisdiction and standardized 'take-it-or-leave-it' contracts. She believes that to give users more control over how their personal data is used, new rules governing the contracts between users and Internet companies are necessary.

This attack on online contracts, terms of agreements and privacy policies using a theory of user control over use of their data has continued into communication research on cloud computing. Due to the relative novelty of this technology, the literature is scarce. However, Bodle (2001) advances many of the same arguments discussed above, applying them to Google's cloud based technologies. He studies the terms of agreement, privacy policies and other privacy-related material of these cloud-based services, and like Fernback and Papacharissi (2007), Cronin (2000) and Radin (2000), concludes that users are not given clear information or the ability to make an educated choice about how and if their data is used. He argues that Google's terms and policies are unclear and contradictory; they frame privacy protection under a discourse of user self-regulation, while at the same time, not giving users clear information to be able to control their personal information (Bodle 2011).

In a similar fashion, legal scholars have attacked terms of agreement and online contracts of cloud computing companies. For instance, Das, Classen, and Davé (2013: 22) argue that "contracts between customers and vendors tend to favor the vendors, which possess greater leverage over the customer." This builds off the argument of Radin (2000) that a reconceiving of contract law for the online sphere is needed. However, they argue that the situation is further complicated by two factors. First, the transnational character of cloud computing makes this difficult to govern and second, the fact that computing technologies are rapidly evolving makes it difficult to develop standard practices for regulating online contracts. Like earlier scholars, they argue that solutions should be oriented around giving customers more negotiating power, more

knowledge and ultimately more control over how their personal information is being used (Das et al. 2013).

While cloud computing scholars have certainly picked up and adapted many of the themes and theories of data privacy that have been around since the early 1990s, they have also highlighted new issues relating to new technologies. The primary challenge of cloud computing is the question of jurisdiction (Jaegar et al. 2009; Office of the Privacy Commissioner of Canada 2011). Because various jurisdictions have different assumptions, approaches and therefore, policies regarding privacy protection (Bennett 1991), governing a technology that is inherently transnational becomes extremely difficult. This is particularly apparent in government reports and white papers on the topic; the Office of the Privacy Commissioner of Canada (2011) as well as the Information and Privacy Commissioner of Ontario (Cavoukian 2008) have published reports and have struggled with the issue of how to regulate data that is constantly crossing borders. It will likely take strong regulation and policies, as well as international and industry cooperation, to solve this issue.

Some other new issues with cloud computing have also been raised in the literature. For example, Bianco (2009) brings forward two closely related issues: data retention and data ownership. Data retention raises questions of how long a cloud service provider can keep and use the data provided by the user, especially in situations in which the user is no longer using that particular service. In other words, if a user deletes their account on a webmail service, can the service provider still use that data for secondary purposes? Data ownership is a similar but deeper concern: when a user exchanges personal data for the use of cloud computing services, who owns the data – the individual

or the service provider who has it stored on their servers (Bianco 2009)? Another important issue involving cloud computing, but also our contemporary technological culture in general is what Cavoukian (2008) calls 'digital identity.' In a culture where individuals actively construct their identities online, and have personal data being stored and used by companies around the world, they open themselves up to the risks of identity theft and fraud (Cavoukian 2008).

It can be seen that critical communications and legal scholars have advanced many ideas about data privacy and cloud computing. The main strengths of this collection of literature is that it develops an excellent outline of the various issues and problems related to informational privacy and cloud computing as well as potential solutions to these issues. Furthermore, communication scholars have adapted philosophical understandings of privacy and applied them in practical settings, which has created good theoretical frameworks for further research on cloud computing. In particular, the distinction between decisional and informational privacy and the theories of restricted access and control are great starting points for researching cloud computing, as well as the governance of Internet privacy and self-regulation of privacy relations. However, as discussed above, I have one major issue with this strand of research: its technological determinist orientation. This standpoint ultimately treats technology as the active determiner of change while users simply become passive recipients of changing privacy values and subjectivities.

Surveillance Studies: Data Privacy, Social Control & Governmentality

The final field of research that I will review – surveillance studies – tries to get away from this theme of technological determinism. Surveillance scholars relate the

collection of personal data to questions about surveillance, security, social control and governmentality. Thus, while communication scholars might look at how cloud computing and Internet technologies create new concerns, social relations and subjectivities, surveillance scholars look to uncover "the deeper motivations and logics behind surveillance" (Monahan 2006: 2). In other words, surveillance scholars do not ask how we can understand, manage and regulate the exchange of privacy for the use of cloud computing technologies, but instead ask why personal data is being collected. In other words, what purposes or techniques of government are being served by the collection of online data? As in the previous sections, there is very little literature that directly addresses cloud computing but rather a broad field that discusses data privacy in general. Thus, I will provide a brief review of surveillance studies approaches to data privacy and finish by discussing the strengths and weaknesses of adapting some of these ideas for an analysis of cloud computing.

Providing a great example of an anti-surveillance approach to data privacy and computing, Andrejevic (2007) explores the meaning of interactivity and how the "promise of interactivity" has developed excitement about new technologies, such as cloud computing and social networks. He explores how many new computing technologies and the associated collection of personal data are framed and justified under a discourse of user empowerment and interactivity (between multiple users and between users and the technology). Using a Marxist framework, he argues that this ideology and discourse of interactivity serves to promote the interests of the corporate elite, develop a 'false consciousness' among users of interactive technologies and essentially maintain the dominant social system while repressing dissent. In other words, the discourse of

interactivity in fact serves to mask the real purpose behind online data collection: market research and to help maintain the hierarchical capitalist system (Andrejevic 2007).

An additional purpose that this rhetoric of interactivity and user empowerment serves is to make users excited about using these technologies, despite some knowledge of personal data being extracted. In other words, the "promise of interactivity" makes users want to be surveilled (Andrejevic 2007). This idea is what Gary Marx (2005) terms "soft surveillance." Marx develops the idea of soft surveillance in the context of DNA and policing, exploring the growth of voluntary DNA samples being given by citizens in order to help police combat crime. However, this idea can be easily applied to the realm of data privacy: as Taddicken (2012) shows, although users are vaguely aware of privacy risks in using web-based services, they readily accept these risks in order to realize the benefits these technologies provide. Soft surveillance is contrasted with "hard surveillance," where users have no choice but to be surveilled, such as under a search warrant (Marx 2005).

As mentioned above, while communication scholars tend to focus on informational privacy (Tavani 2008), surveillance scholars explore decisional privacy at a deeper level. While they are still concerned about the exchange, control and ownership of personal data, surveillance studies look at the deeper motivations of why this data is important – the ability to make independent choices. For example, Fuchs and his colleagues (2012) make the theoretical distinction between economic and political surveillance, although elsewhere Fuchs (2012) argues that on an empirical level it is difficult to distinguish between them. Economic surveillance is typically by corporations to influence consumer behaviour and decisions, while political surveillance is typically

done by states in order to police behaviour and govern political dissent (Fuchs et al. 2012). Thus, it can be seen that surveillance studies are not simply concerned with the exchange of personal information, but the reasons behind the collection of this data and how it used for social control and influencing economic and political decisions.

A major benefit of surveillance studies is that scholars in the field have completed numerous detailed empirical case studies highlighting these ideas of economic versus political surveillance and decisional privacy. The remainder of this section will review some important case studies of economic surveillance, followed by case studies of political surveillance. Allmer (2012) argues that economic surveillance typically takes two forms: surveilling consumers or surveilling the workplace, corresponding with the consumption and production spheres of a capitalist economy. Using Internet surveillance to monitor production involves situations such as employers monitoring emails and computer usage in order "to document and control workers' behaviour and communication to guarantee the production of surplus value" (Sandoval 2012: 137). In the sphere of consumption, economic surveillance is aimed at gathering information about consumers in order to more efficiently advertise and influence users' behaviours and preferences (Sandoval 2012). For example, in performing a content analysis of social networking sites' privacy policies, Sandoval (2012: 165) concludes that these agreements "are designed to allow the owners of these platforms to exploit user data for the purpose of capital accumulation."

However, Andrejevic (2012) argues that economic surveillance of consumers is not simply a practice of market research but is what he terms "consumer exploitation." He expands the Marxist notion of exploitation outside the realm of the workplace and

into the realm of consumption. Andrejevic (2012) explores the idea of 'user-generated value' and 'user productivity' and argues that in using web-based technologies, users are creating value for corporations in terms of detailed behavioural data. In other words, users are creating surplus value and a more valuable product for the corporation without their labour being acknowledged or rewarded. In the end, consumer exploitation has a double effect:

> "First, consumers are not generally paid for the know-how, enthusiasm, and social cooperation… that they contribute to the manufacturing process of marketable commodities. Second, customers typically pay what the marketing profession calls a 'price premium' for the fruits of their own labour" (Zwick, Bonsu and Darmody 2008).

Furthermore, Andrejevic (2012) argues that, similar to workplace exploitation that Marx observed in the early modern factory, digital consumer exploitation has a coercive element – not in a direct, violent sense but rather in the sense that nearly everything we do in modern society is mediated and documented by online surveillance technologies.

Andrejevic (2007) exemplifies these ideas and the complex nature of economic surveillance using digital technologies using the case study of TiVo and 'interactive' television. While it is not directly applicable to cloud computing, this case study highlights these surveillance studies' concerns about data privacy and the ideas of economic surveillance and consumer exploitation. Andrejevic (2007) discusses how TiVo, while giving consumers more freedom and choice in television viewing habits, also gives corporations detailed information on viewing preferences and behaviours. He discusses how users are ultimately doing work for the corporation by telling them which shows they like to watch. He calls this a "duty of interaction," arguing that users are "required to take on a broad array of interactive responsibilities" (Andrejevic 2007: 144).

This allows for more targeted, efficient and effective advertising to each individual user. Thus, echoing the concerns about decisional privacy discussed above, Andrejevic argues that the "duty of interaction" placed on the user allows corporations to generate surplus value from consumers and ultimately have greater influence over their economic decisions.

While economic surveillance is about monitoring employees and consumers and is discussed by surveillance scholars under the rhetoric of exploitation, political surveillance is about monitoring citizens, both for monitoring political views and policing (Fuchs et al. 2012). Here, the purposes behind surveillance are largely framed using Foucault's concept of governmentality, as "it deals with altering a subject's behaviour to coincide with the norms, practices, and laws of a society" (Arditi 2012: 172). For example, Fuchs and his colleagues (2012) argue how digital surveillance technologies are often used in policing citizens, particularly when it comes to issues of national security and terrorism. However, at the same time, surveillance technologies can also be turned back on officials, such as the filming of police brutality in the Rodney King case. By showcasing the two-way nature of surveillance technologies, Fuchs and his colleagues (2012) are highlighting how these technologies help govern all citizens, including officials, to conform to the laws and norms of the society. However, they do point out that it is not a one-to-one relationship between citizen and official surveillance but instead the use of political surveillance reflects asymmetrical power relations (Fuchs et al. 2012).

Andrejevic (2007) provides two case studies of political surveillance using Internet based technologies: 'interactive' war and 'interactive' politics. In talking about

surveillance and war, he draws parallels between the "marketing of interactivity and the advertising campaign for readiness" (Andrejevic 2007: 162) in the context of the war on terror. While acknowledging the differences between economic and political surveillance, and between the micro scale of individual social media use and global politics, Andrejevic (2007: 163) argues that in both cases the discourse of interactivity is used "as an information gathering strategy and as an invitation to identify with the imperatives of those in positions of power, either cultural or political". In other words, citizens are asked to take an active role in the war by staying up to date with news and more importantly, being involved in the lateral monitoring of others (Andrejevic 2007). Government agencies are also involved in this monitoring[7] in order to police political dissent and ensure active citizen participation (Andrejevic 2007).

In his case study on 'interactive' politics or 'iPolitics', Andrejevic (2007) explores campaign strategies from the 2006 midterm elections in the United States. He shows how both political parties began using Internet surveillance techniques to monitor and influence citizens' political behaviour, in much the same way corporations are involved in consumer surveillance. In the same way that corporations use data for targeted advertisements aimed at increasing brand loyalty, political parties were able to mine data in order to do the same to increase party loyalty. Not only does this show the close connection between economic and political surveillance, but it led Andrejevic (2007) to critique the popular argument that "Web 2.0" is democratizing the Internet by providing a space for non-mediated public opinion. Instead, he argues, it is becoming a new space for political surveillance.

[7] For example, in the U.S., the NSA's PRISM program is a mass secret data collection program for the purposes of surveillance and security (Gellman and Poitras 2013).

While these case studies try to think about economic and political surveillance separately, in practical situations the two reinforce one another since the nature of the political economy is that the two spheres work together harmoniously (Fuchs 2012). An excellent case study that highlights this idea, as well as giving some insights into how this surveillance literature could potentially be applied to cloud computing, is provided by David Arditi (2012). Arditi discusses the surveillance of both legal and illegal music downloads. He argues that the cooperation between the music industry, law enforcement agencies and digital music stores in surveillance of music consumption serves two mutually reinforcing purposes. First, it gathers data on consumers' tastes, preferences and behaviours. Second, it polices illegal music downloads (or piracy). Thus, in employing both economic and political surveillance methods simultaneously, the music industry is essentially "disciplining the consumer" into consuming legitimate, legal and profit-generating digital music (Arditi 2012).

Additionally, Arditi's case study highlights some interesting points for a study of cloud computing. He argues that when the music industry and politicians began their crack down on peer-to-peer (p2p) networks, they implied that all uses of these services were illegitimate. He argues they ignored legitimate uses of p2p networks and assumed all file sharers were criminals illegally downloading music (Arditi 2012). This is contrasted with new cloud computing services whose benefits, as discussed above (Benkler 2006), are often framed in terms of co-production and file sharing within the workplace. Hypothetically, they could be used for the same uses as early p2p networks such as Napster – to pirate and share music. However, it would interesting to see the difference between p2p networks and cloud computing services and to compare how

political and economic powers and surveillance technologies construct, monitor and influence users of these two Internet-based technologies.

In thinking about ways to apply surveillance studies on data privacy to cloud computing more specifically, one idea is notably absent: the jurisdiction issue. As discussed above, cloud computing always involves centralized data centers, often in other jurisdictions with more favourable corporate laws. Thus, an important topic for surveillance studies would be to look at the intersection of international law, data centers and surveillance. However, most of the surveillance literature available tends to look at data privacy in a local, domestic setting[8]. Some surveillance scholars however have tried to address ways to conceptualize surveillance across international borders. Christensen and Jansson (2012), for instance, argue that using Bourdieu's concepts of the field is preferable for discussing online spaces that cross national borders. This echoes a similar argument from Barry (2001), who states that a challenge in governing a technological society is identifying, setting up or governing "technological zones". These refer not to zones defined by political, legal, or physical boundaries, but are "zones formed through the circulation of technical practices and devices" (Barry 2001: 3). Thus, while surveillance scholars have not directly addressed the jurisdictional issue of cloud computing, they have begun to develop concepts and theoretical approaches to study the changing nature of data privacy.

Despite this one omission, the surveillance literature provides a novel way of thinking about data privacy as well as numerous detailed empirical case studies. By asking questions about the purpose and motivation behind surveillance technologies and

[8] This could be an effect of the surveillance studies field ultimately going back to Foucault (Allmer 2012). It is not uncommon for Foucauldian literature to be biased towards the local, domestic or "microphysics" of power (Walters 2012).

exploring the power effects of online data exchanges, surveillance scholars are able to avoid the technological determinist assumptions that run through the communication and legal literature. Additionally, this approach allows scholars to connect issues of data privacy with larger social, political and cultural issues, such as Andrejevic's (2007) case study of the war on terror or Fuch's (2012) critique of modern political economy. Thus, while both communication and surveillance scholars problematize the changing nature of privacy in relation to Internet technologies, communication scholars look to address its underlying causes while surveillance scholars look to address its effects.

Despite these strengths of the surveillance literature, there is potentially one drawback to this field of research, namely the assumption that new technologies repress users and society. There is a tendency to privilege privacy and assume the existence of a homogenous cultural value of privacy protection. In other words, all the research discussed above naturalizes certain privacy values; it assumes that all users do not want their data exposed. However, as Taddicken (2012) shows, users' privacy values are variable and many users, despite being aware of the surveillance techniques affecting them, willingly accept sacrificing their privacy in order to use these technologies. Ultimately this has a similar effect as the determinist assumptions of the communications research: it treats technology as active while users as passive. Users have a 'false consciousness' in that they are being duped in using new technologies while their essential social rights or interests – their private information – are being repressed.

This tendency is noticed within the field of surveillance studies with some authors calling for alternatives. Trottier and Lyon (2012) caution that surveillance studies tend to be "preoccupied with the Orwellian and the panoptic" forms of surveillance.

Albrechtslund (2012), while not dismissing these forms of surveillance, argues that surveillance scholars also need to accept more neutral forms of surveillance. He coins the term "participatory surveillance" to refer to "the social, playful, and potentially empowering aspects of surveillance" (Albrechtslund 2012: 189). These ideas might help surveillance scholars get away from naturalizing certain privacy values and a particular conception of the subject under surveillance.

Conclusion: Reimagining the User and Human Agency

Thus it can be seen that there is no perfect 'one-size-fits-all' approach to understanding data privacy and cloud computing. Each field I have discussed has its strengths and weaknesses. The business and economic literature does a great job of highlighting the benefits of cloud computing but reeks of technological fetishism, largely ignoring the potentially harmful consequences that these technologies can have to individual privacy and personal data. Critical communications, legal and policy studies offer the most extensive research on the topic, adapt philosophical understandings of privacy into real world practicalities and offer many innovative solutions. However, this field of research is largely technologically determinist, creating some issues for sociological research. Lastly, surveillance studies offer a novel approach to data privacy, focusing on questions of power and social control and the motivations underlying digital surveillance technologies. While this approach allows the field to avoid the determinist assumptions of communications research, it also naturalizes a particular view of the subject under surveillance and their privacy values.

What these various drawbacks have in common is that they reduce the role of users and of human agency. On the one hand, new technologies are seen to determine social change. However, where do these technologies come from if not from individuals acting as agents? On the other hand, technology is seen as repressive – it is used to infringe on privacy, understood as a natural, homogenous social trait. However, this does not capture the complexities of data privacy and the fragmented, shifting, contextual and contingent nature of privacy or the agency of users and how they interact with technology. In both traditions, users are passive; in the determinist view they are simple recipients of technological change, while in the repressive view they become dupes who have their privacy repressed by a new technology. To fill this gap, I believe the challenge is to adapt concepts and ideas from each of these above fields, as well as other theoretical traditions, in order to fully capture the complex nature of privacy and the relationship between users and technology.

While this project does not hope to offer a complete solution to this challenge – my goals are much more modest – I do hope to offer some insight into the relationship between cloud computing and its users in a way that looks at and grants agency to both parties. I find that trust is one lens through which this interaction can be studied; users actively trust other parties, while technologies work to promote their durability, reliability and trustworthiness. However, I am not alone in this thinking; several scholars have recently turned to the question of trust, rather than privacy, as the primary conceptual lens in understanding cloud computing. For example, Ryan and Falvey (2012) argue that users of cloud computing must change conceptions of trust to adapt to new technologies. They argue that users have a "if I can see it, I can control it" mentality which has led to

initial distrust of cloud computing; however, users must change this perception in order to adapt to the new technology (Ryan and Falvey 2012). This idea is also advanced by Grodzinksy and Tavani (2011), arguing that for the benefits of cloud computing to be realized, users must trust the service provider to secure and protect their data and make it readily accessible for the user.

Other scholars have discussed the relationship between trust and information and communication technologies, and have made attempts to conceptualize the nature of trust and the role it plays in informational privacy protection. For instance, France Belanger and her colleagues (2002) examined early e-commerce companies and their perceived trustworthiness. They found that consumers valued security features above all when judging the trustworthiness of a company and more notably, that the perceived trustworthiness of the company precedes consumers outsourcing private information such as a credit card number (Belanger, Hiller, and Smith 2002). In other words, privacy follows trust. Metzger (2004) and Chellappa and Sin (2005) take a similar view. Trust is an important antecedent to self-disclosure; users will not disclose personal information unless they trust that it will be respected (Metzger 2004). Furthermore, online consumers' trust in vendors is an important criterion for accepting the trade-off of private information for personalized services (Chellappa and Sin 2005).

Bansal and his colleagues (2010) take an opposing view; they find that trust is often a product of user personality and previous experiences with privacy concerns or protection. In this case, trust follows privacy. Trust is still necessary to disclose personal information; however, the decision to disclose personal data is not simply a process of weighing an Internet company's perceived trustworthiness beforehand. Trust is rather

complex and composed of several factors, including the personality and behaviours of the user, and is built through interaction with the Internet company and other parties over the course of one's life. Elsewhere, Bansal argues that trust is highly dependent on context and that individuals' trust affects how they react to privacy concerns (Bansal, Zahedi, and Gefen 2008).

As these studies show, trust is an important mediator between privacy concerns and self-disclosure. I argue that it is also an important conceptual lens for understanding privacy in a way that offers a break from the determinist or repressive views of privacy, and allows for research to reimagine user agency in relation to these new technologies. However, more work on the role and meaning of trust is needed. In the following chapters, I attempt to contribute to this literature on trust by offering an alternative theoretical approach to understanding trust using a case study of Dropbox.

3 Deconstructing Privacy: Theory and Methods from Actor-Network Theory

In the previous chapter, I concluded that there is potentially a gap in the literature on data privacy. On the one hand, there is the view that technology – such as cloud computing – is determinist of social relations. On the other hand is the view that technology is repressive of social relations. Both of these views leave little room for the agency of users; they simply become placeholders for technological advancement or dupes. However, I have argued that literature on trust is one growing area of research that can offer a break from this determinism-repression duality. In this chapter, I propose to incorporate actor-network theory as an alternative approach to further the literature on data privacy and trust in a way that respects the agency of users. However, this is not to argue that the approaches discussed above are valueless; as discussed previously, I believe the communication studies and surveillance research on data privacy have outlined some important understandings of the nature of privacy and the rationales behind Internet technologies. My argument is that actor-network theory can add some important insight into understanding the relationship between data privacy and user subjectivities, particularly using the ideas of the 'co-production' of technology and society. In other words, these approaches help understand the complexities of users' values and perceptions regarding privacy.

I will advance this argument as follows. First, I will provide a brief introduction to actor-network theory (ANT) and some of its central ideas. The goal of introducing these concepts will be to highlight how ANT conceives of the co-production of society and technology, distancing itself from other approaches that privilege either the social or the technical. Second, I will discuss a particular critique of ANT from Susan Leigh Star

(1991). This critique is useful not because it rejects ANT, but rather because it follows many of the main assumptions and allows this theoretical approach to develop a more nuanced understanding of users. It could be argued that this critique of ANT actually became a central text of this theoretical approach and has influenced later ANT work on users[9]. Third, I will delve into more detail on a few ANT concepts that are of particular important to this project, namely scripts/de-scription (Akrich 1992; Akrich and Latour 1992), black boxes (Latour 1987; 1991) and breakdowns. Finally, working from the assumption that ANT is not a theory per se but rather a set of conceptual tools, I conclude by outlining how this approach can be methodologically applied in my project on cloud computing, trust and data privacy.

Actor-Network Theory: A Brief Introduction

Actor-network theory is a material-semiotic approach. It treats natural and technological phenomena (materials) as well as cultural and ideological phenomena (semiotics or ideas) to be of equal analytical importance (Law 2009). In other words, it tries to avoid binary distinctions such as nature/culture or social/technical. In fact, John Law (2009) argues that using the term material semiotics is preferred to actor-network theory as it covers a larger and more diverse field of theoretical and empirical traditions. This material semiotic approach is "not a creed or dogma" (Law 2009: 142) but represents an alternative way of thinking about the relation between social and technical relations.

[9] For example, the work of Madeleine Akrich (1992; Akrich and Latour 1992), which I cite extensively in this work, shares some of the central assumptions of Star (1991), particularly a respect for human agency and individual difference.

Central to this idea of looking simultaneously at materials and semiotics is the methodological concept of symmetry. Originally appropriated by Callon (1986), symmetry refers to the process of explaining natural or cultural phenomena using the same – or symmetrical – tools and language. In other words, an analyst should not have any a priori conceptions of what is natural or cultural, of what is technical or social, but rather look at how certain objects or subjects are constructed and mobilized as natural, technical, or social beings. In other words, ANT scholars "treat everything in the social and natural worlds as a continuously generated effect of the webs of relations within which they are located" (Law 2009: 141). For a study of cloud computing and data privacy, this methodological approach could be useful in avoiding the binary opposition of determinism-repression I have discussed above. I want to start my research without a conception of whether privacy is a social value that is being repressed or a technically determined value, but instead look at how it is contingent, contextual and involved in a complex web of relations.

ANT can be said to be about two related but distinct process: first, how these heterogeneous elements – composed of humans and non-humans – are enrolled into a network; and second, how the heterogeneity of this network is reduced to a homogenous, durable and stable technological artefact, standard or process (Latour 2005). A word on each of these two processes is necessary. John Law (1987) dubs the process – the building of a heterogeneous network – as "heterogeneous engineering". The success or failure of an innovative technological artefact or idea is dependent on the heterogeneous engineering and the building of a network (Law 1987). For example, the heterogeneity of cloud computing has already been alluded to: cloud computing is not one static

technological artefact but rather an idea that holds together a range of new computing hardware and software, as well as users, governments, programmers, data centers and others. This project focuses on how one such actor – the end-user of cloud computing – might be enrolled into this heterogeneous network. More specifically, it is about how one aspect or fragment of this end-user – their perceptions of privacy – are translated, negotiated and potentially enrolled into this network called "cloud computing".

Thus, ANT scholars look at how actors – persons, organizations or technological artefacts – enrol allies into a heterogeneous network (Latour and Woolgar 1979; Latour 1988; Callon and Law 1982). Any 'actant' – human or non-human – that can act or create effects on another entity can be considered an actor in this approach (Latour 1992; 1991). An important concept in understanding the enrollment of heterogeneous allies into a network is the idea of translation (Callon 1980; 1986). Michel Callon (1980) develops the idea of the translation of interests to explain how new actors are enrolled into the network; the terminology of 'translation' is important as it highlights how interests are not necessarily imposed or coerced through relations of domination, but instead how interests are subtly realigned to be in harmony with the actant. Thus, this process of translation (or displacement) can be resisted and negotiated, in which case the intriguing empirical question becomes how this negotiation unfolds. It is the nature of this process – how the translation of privacy interests is negotiated – that is of central importance to this project. In short, this project looks at how the end user, or more precisely a fragment of the end user – their privacy values, is enrolled into this network through the exchange of 'privacy' for use.

The second process involved in the building of a network is that of stabilization, or how the heterogeneity of the network is reduced to a homogenous set of standards, artefact or technological practice. Essentially, this involves looking at how heterogeneous actors and viewpoints become aligned through the process of translation. In other words, ANT scholars want to look at how precarious networks become stable and durable. Latour (1991) argues that technologies are the materialized reality of stabilized network; it is society and social relations under different material forms. All technologies involve social relations; however, once a technical practice or artefact becomes mobilized as 'technology', its heterogeneity or the 'social' is reduced.

ANT scholars tend to examine controversies as sites of analysis in which heterogeneous actors and viewpoints are not aligned (Latour 2005). By looking at how actors enrol allies and align interests within a controversy, they are essentially looking at the closure of a controversy. Spokespersons align viewpoints and thus erase the heterogeneity of a network. Instead of looking at the 'social factors' to explain phenomenon within groups, ANT scholars look at how groups are formed (Latour 2005); how are controversies closed and heterogeneous actors aligned? Technologies are representations of heterogeneous networks that have been aligned, or controversies that have been closed: "it is as if we might call technology the moment when social assemblages gain stability by aligning actors" (Latour 1991: 129).

With this understanding of controversies, stabilization and technology comes the idea that technical standards are a power effect. ANT scholars do not want to look at how power relations and powerful actors exert their power in order to enrol actors in their network or create technical standards that are to their advantage. Instead, "power and

domination are words given to those stabilizations and not an account of their coming into being" (Latour 1991: 129). When a heterogeneous network stabilizes, it creates standard viewpoints, practices and interests. Technical standards are thus the representation of this power effect. When technical standards develop, controversies are closed: "when actors and points of view are aligned, then we enter a stable definition of society that looks like domination" (Latour 1991: 129). In other words, technical standards remove issues from a 'space of disagreement' (Barry 2002). Standardized socio-technical networks become next to impossible to contest or resist (Star 1991). For example, my project will look at whether, and if so, how user subjectivities regarding privacy are standardized. Is there a standard view of privacy that users must adhere to, or are cloud computing networks "a highly unstable and negotiated situation in which domination is not yet exerted" (Latour 1991: 129)?

The value of asking such questions and employing such a method is to highlight the 'co-production' of technology and society. The "idiom of co-production" (Jasanoff 2004) does not simply argue that technology has a causal effect on society and vice-versa, but rather tries to open up ways of thinking about how the two are inherently interconnected in complex, fragmented and contingent ways. Technology is not conceived as an objective application of knowledge nor as a simple reflection of social or political environments. By treating either the 'technical' or the 'social' as an a priori structure that can exert effects grants them an unquestioned and problematic agency (Jasanoff 2004; Latour 2005). In other words, it treats technology or society as unquestioned entities; co-productionist accounts are interested in exploring both these

entities and highlighting the complexities and associations that make technologies and societies possible.

An account of data privacy that sees advances in computing technology changing the nature of privacy and user subjectivities takes these technological advances for granted without questioning the translations, associations and heterogeneity involved in computing advances. The other, more common view that might highlight the social and political relations involved in computing technologies by exploring how they repress privacy – an inherent social right or interest – is equally problematic. It takes privacy for granted and does not question the contingencies, negotiations and multiplicities of privacy values and user subjectivities. Considering privacy as a natural social right or a technological value treats it as an entity outside and independent of users. A co-productionist approach, on the other hand, only looks at privacy in terms of how it is associated and mobilized in action. Privacy is not an a priori right, value or entity but only exists in the specific moments it is conceived and employed. The important question for a co-productionist approach then becomes *how* privacy is conceived and employed at these specific sites.

Looking to the Margins: Star's (1991) critique of ANT

These concepts outlined by ANT are conveniently summarized in Bruno Latour's (1987) short methodological principle: "follow the actors". Latour is referring to how the social scientist should observe how actors enrol allies, displace and translate interests, build a heterogeneous network and stabilize this network. This principle – as the methodological crystallization of many of ANT's main assumptions – has not been without critics. Most notably, it has been challenged for being an 'executive approach'

(Star 1991; Clarke and Montini 1993). It only focuses on how powerful actors build networks and thus neglects user agency and more importantly, non-users – those on the margins of these networks (Star 1991). In this following section, I will expand on such critiques of the ANT approach. However, it is important to note that these critiques do not necessarily dismiss ANT; often, they work from the same co-productionist assumptions and build upon this body of theory. I will discuss the critique levelled by Star (1991) and feminist technology scholars that aim to bring questions of marginality, affinity and multiplicity into an ANT account. ANT has been reshaped and renegotiated amidst such critiques, resulting in a vibrant, co-productionist, 'beyond actor-network theory' (Law and Hassard 1999) body of literature that allows for a complex understanding of user subjectivities.

Star (1991) begins from the observation that the 'executive approach' of ANT ignores non-users and more importantly, users on the margins of networks. She argues that even when networks have stabilized, there will still be marginalized users – users who do not necessarily fit in the stable network and might 'slip between the cracks' of multiple standard networks. Users are treated as whole, static entities that are either enrolled into a network or not; thus, the executive approach omits questions of multiplicity and marginality. A user is a node in the network, while the executive approach looks at the processes by which this node is connected with other actors in the network. It does not encapture how users are split, dynamic and may be simultaneously enrolled in multiple, often contradictory, networks (Star 1991). It helps us think about the heterogeneity of networks, but not the heterogeneity of users themselves.

This critique of ANT essentially employs a view of the subject as fragmented and multiple. The fragmented nature of subjectivity and individuality has been a common theme in social thought; for instance, Georg Simmel assumes the fragmented image of human experience: "we are constantly circulating over a number of different planes, each of which presents the world totality according to a different formula; but from each our life takes only a fragment along at any given time" (Levine 1971: xxxviii, translated from Simmel 1918). This highlights an early sociological approach that aims to focus on the intersections between multiple subject positions. However, this theme accelerates in social thought with and the advent of 'postmodern' thought and the collapse of metanarratives[10]. A central tenet of postmodern social thought is the move away from the "view of the individual as a separate, autonomous, and unitary self [in favour of] a self who occupies simultaneous axes of gender, class, race, and sexuality" (Seidman 1994: 11).

It is this conception of the individual and subjectivity that Star (1991) employs in critiquing the executive approach of ANT. In particular, she is appropriating concepts from two sociological traditions that conceptualize the individual as fragmented: ethnomethodology and feminism. These approaches do not necessarily refute ANT but in fact can add and build upon its discussion of users, subjectivity and power relations, as evidenced by Star's analysis. Ethnomethodolists focus on how individuals create meaning in social interaction (Hibbert 2009). Central to this approach is the idea that in social interaction, individuals employ a multiplicity of meanings and selves.

This idea is further shown by how Star (1991) employs a feminist understanding of the subject and engages with the feminist technology studies of Donna Haraway. Both

[10] This shift in thinking is discussed in, and often attributed to, Lyotard's (1984) *The Postmodern Condition*.

Star and Haraway use the concept of affinity rather than identity to denote a user's membership in a group. Identity is seen as a static, all-encompassing description of one's group membership, whereas affinity allows for the multiple, shifting and contextual aspects of group membership (Haraway 1991). In other words, affinity allows one to understand how subjectivities and experiences are fragmented along multiple axes.

In Star's (1991) understanding of ANT, this is manifested as users being simultaneously enrolled in many and often contradictory networks. She uses the metaphor of the 'zero point' to refer to the moments when users are simultaneously enrolled in multiple networks, or are not enrolled at all but ambiguously fit between multiple stabilized categories (Star 1991). In other words, they do not accept nor reject the user scripts of any of the networks in question, but rather ambiguously float between these networks. Standard networks attempt to standardize users, or in other words, reduce their marginality (Star 1991). As the heterogeneity of a network is reduced and it becomes more stable and durable, it more clearly delineates the boundary between user and non-user. By maintaining their marginality, their non-standard position, or their zero point, users are exercising a means of resisting standard categories. However, a hypothetical network whose heterogeneity is completely reduced will not have such marginal users; users are either a part of the standard category or they are not. As the network becomes more homogenous, users become more homogeneous; they lose their sense of individual difference. Thus, Star (1991) argues that look at the 'zero point' of users can help highlight the strength of a given network; at the moment of action, which script is the user accepting, rejecting or negotiating? In other words, when users act, to which network(s) they belong?

The Human-Technology Relation: Scripts, Black Boxes and Breakdowns

It must be stressed that this conception of users and multiple selves is not incompatible with ANT, but by starting one's analysis with the executive actor rather than the marginal actors, the multiple and fragmented quality of user subjectivities is ignored. In short, Star's (1991) critique could be said to mark a shift towards a more user-centric approach in the history of ANT. In the following years, ANT scholars further developed concepts and ideas to look at the relationship between users and technologies. In particular, they have advanced two concepts that help us understand how users might be enrolled into a socio-technical network – how their viewpoints might be displaced, translated, or aligned: scripts and configuration. Like the film script, 'user script' in ANT refers to how human actors and technical objects are expected to behave (Akrich 1992; Akrich and Latour 1992). As posited by Akrich (1992), every technical object has a script which defines the relationship between users and other users, or between users and the artefact. In other words, artefacts "delegate specific competencies, actions and responsibilities to users" (Oudshoorn and Pinch 2003, citing Akrich 1992). Scripts are involved in the aligning of user interests; they are involved in the construction of user subjectivities. Thus, in using ANT to look at cloud computing and privacy, we would have to look at the script of a cloud-based artefact, piece of software or service. What understandings, values or actions regarding privacy does cloud computing prescribe on users?

Another way of understanding this idea is by using the approach of Steve Woolgar (1991) and the concept of configuration. Woolgar (1991) uses a "machine as text" metaphor to show how particular uses of a technology are configured. He defines

configuration as "defining the identity of putative users, and setting constraints upon their likely future actions" (Woolgar 1991: 59). The designers and engineers are the 'authors' of the text, while the users are 'readers'. Similar to the concept of script, this user configuration involves prescribing and outlining limits to the uses and meanings a technology can have, but leaves room for some interpretation and agency from the user. However, the value of Woolgar's approach is that by using the textual metaphor, he is highlighting the discursive power of technological artefacts. They do not coerce certain uses, but through discursive practices subtly shape and govern certain uses.

By aligning viewpoints, enrolling actors into a network and prescribing or configuring user subjectivities, an actant essentially becomes a spokesperson for other actors. It is important to look at who speaks on behalf of whom and how and why this representation occurs (Callon 1986). For instance, a scientist can become the spokesperson for the natural phenomenon they are studying (Latour 1987), or in Woolgar's (1991) example, computer engineers become a spokesperson for users through configuration. Thus, in short, my project will ask how a technological company or artefact can become a spokesperson for its users' subjectivities – their values, actions and understandings of privacy. This is similar to van Oost's (2003) usage of Akrich's concept of script; she coins the term "gender script" to look at how a technology might prescribe an aspect of users' subjectivities – gendered understandings and actions. Similarly, I also want to look at how fragments of user subjectivities – privacy and trust values – are prescribed; it could be said that this project will look at a technology's 'value scripts'.

However, ANT scholars have conceded that simply looking at the texts and discourses offered by technologies is insufficient. Akrich (1992) realizes that just focusing on scripts and prescribed use reinforces a technological determinist view, and wants to incorporate the agency of users' into her analysis. Thus, she argues that analysts "have to back and forth continually between the designer and the user, between the designer's projected user and the real user" (Akrich 1992: 208-9). This concept of 'description' (Akrich 1992) refers to how users interpret and create their own meaning from the script offered by a technology – how they adapt their own uses. These meanings and uses are not necessarily in agreement with the prescribed use of a technology; in this case, they would constitute what Latour (1991; 1992) calls an 'anti-program'. Thus, in this project, the notion of description is useful in that it expands our understanding past the idea that this new technology leads to a change in privacy values. It helps to avoid falling into the trap of attributing a homogenous set of privacy values to users of cloud computing. These concepts instead highlight the mutual shaping of users and technology and the multiple and flexible nature of privacy values.

Another useful metaphor that helps illustrate the relation between users, technologies and scripts is Latour's (1991) usage of the term 'black box'. The black box refers to an entity or artefact that is encased such that its internal workings are hidden and taken-for-granted. In other words, once a network stabilizes and its heterogeneity is reduced to common standard, artefact or practice, it is black boxed. The heterogeneity of actors has been erased, viewpoints aligned and controversies closed. Users *trust* that the black boxed technology will behave accordingly so long as they adhere to its user scripts; the technology will behave if they, the users, do. The role of the analyst thus becomes

'opening the black box' (Latour 2005; Winner 1993) or in other words, questioning those internal workings, user scripts and heterogeneities involved in every technological network that have since been reduced and erased.

The internal workings of a black boxed technology are only questioned when they go wrong, when they misbehave (Latour 1992). In other words, the taken for grantedness of a technology disappears when it *breaks down*. These instances of breakdown thus become important empirical sites. Akrich (1992) argues that the analyst should look to instances in which the inside – the black boxed technology and its user scripts – does not line up with the outside – users and their description – as sites in which script and description become observable. When a technology is stable and black boxed, its user scripts are taken for granted; the inside and the outside of the technology are aligned. However, when users have the expectation that a technology will behave in a certain way and the technology fails, the expected behaviour of the user that is typically black boxed, unquestioned and taken for granted becomes questioned and negotiable. In other words, when the user can no longer trust the technology to behave appropriately, the previously stable actions and behaviours delegated to users themselves become destabilized and contested.

Applying ANT principles to cloud computing and data privacy

To summarize what has been said so far: ANT looks at how associations are made, how actors enrolled into a heterogeneous network and how such a network might stabilize. However, Star's (1991) critique of the 'executive approach' of ANT brings attention to the need for a more nuanced understanding of users and how they interact with standardized technologies. My project attempts to engage with and bring cloud

computing and data privacy into this theoretical framework. This serves three closely related purposes that help work towards my goal of understanding cloud computing, trust and data privacy in a manner that keeps user agency in mind. First, by treating cloud computing as a network, I am attempting to highlight its heterogeneity; it is not a technological entity that determines or represses privacy, but rather it is a heterogeneous assemblage comprised of several associations, which may be more or less stabilized. The fact that cloud computing is treated as a technological entity in the literature – both academic and popular – which suggests that it is somewhat stabilized. However, my project will explore how its use might still be negotiated.

Second, by employing an ANT approach, this project attempts to look at the nature of the privacy exchange discussed throughout the literature as a process of enrollment. Users exchanging privacy for the use of cloud computing processes can be understood as an effort to enrol users into this heterogeneous network. However, this is closely related to the third purpose for using this theoretical approach, here specifically engaging with Star's (1991) cautions against the executive ANT approach and Akrich's (1992) concepts of script and description. This project specifically wants to understand the relationship between users of cloud computing and the technology itself. The value of Star's (1991) analysis is essentially to show how stable networks and standardized uses of a technology marginalize certain user experiences and subjectivities. Akrich provides the methodological tools and concepts to observe the varied experiences of users (description) and the standard stabilized scripts of a technology; we can observe the relationship between the ideal, imagined user and the actual user(s).

Thus, instead of seeing privacy as an inherent social value that is being exchanged for use of the cloud computing service, this project works from the assumption that privacy values are multiple and contextual. Following Star (1991), I will look at which understandings of privacy are employed in the use of the technology. Thus, my project will explore whether there are multiple and fragmented subjectivities regarding privacy, the attempts of the cloud computing network to further standardize users' privacy values and the implications of this standardization.

Another way to frame this challenge is by using the concept of 'subject networks'. Similar to Star's critique of the 'executive approach' of ANT, the concept of subject networks argues for starting one's analysis not from a powerful actor and their building of a network – their heterogeneous engineering' – but rather from the point of view of the user, the subject (Oudshoorn and Pinch 2003). In what network(s) are they enrolled? How have they become enrolled in these networks? For example, Ingunn Moser (2000; Moser and Law 2001) has explored the 'subject networks' of persons with disabilities to explore how they are enrolled into several socio-technical networks and the connections this has with identities and subjectivities. Similarly, in the following chapters, by starting from the point of view of the subject, I will explore how the users of Dropbox might be enrolled in several networks and how this might affect their subjectivities or in other words, their values, understandings and actions related to privacy.

In sum, ANT has traditionally aimed to deconstruct the heroic actor of a network (Law 1991); however, Star's (1991) critique highlights the importance of deconstructing the end user of a network. This is what the remainder of this project will be dedicated to accomplishing: deconstructing the user of cloud computing in order to highlight the

contingent, contextual and fragmented nature of their understandings and values regarding privacy. In other words, it is dedicated to providing one way of understanding the relationship between a technology and its users that maintains a place for user agency and individual difference.

4 Dropbox's User Scripts

In the previous chapter, I have argued that one way to fill the gap in the literature of exploring what privacy is and how users' privacy values and subjectivities are negotiated is to use an actor-network approach, specifically employing the concepts of scripts, description, and breakdowns. In this chapter, I begin tackling the first of these concepts in relation to cloud computing, as represented by the case of Dropbox. Dropbox is an excellent example of a cloud computing service which allows users to store files, folders and programs on an Internet storage system, to be accessed whenever and wherever they please. I will use the Dropbox example for three reasons. First, as compared to other popular cloud services such as those offered by Google, there is relatively little existing research on Dropbox. Second, Dropbox offers a significant amount of rich 'official' discourse on privacy through privacy policies, terms of agreement and online company blog posts, as well as a vibrant online support community with several user questions and concerns regarding privacy. Lastly, and most importantly, Dropbox has been subject to a few privacy and security fiascos over the past two years. In 2011, Dropbox suffered a technical bug which temporarily allowed anyone to login to any Dropbox account using any password (Harbison 2011). In 2012, a Dropbox employee was hacked, providing the hacker with several account names and passwords (Samson 2012). Finally, in 2012, Dropbox was named as a potential future participant to the NSA PRISM program (Gellman and Poitras 2013; see footnote 7). These three events, in actuality or hypothetically, put users' personal data at risk to be accessed by unsolicited parties and highlighted the privacy risks of cloud computing. In essence, they represent the idea of breakdown from ANT; they provide empirical cases in

which a technology that is more or less taken for granted stops functioning as expected, resulting in a questioning of its purpose and 'opening the black box'. Thus, Dropbox represents a case study that has the opportunity to be different from existing research, relevant and rich in data regarding privacy.

In short, I will explore how Dropbox enrols users into its network. I ask what sorts of scripts Dropbox inscribes on its users. What sorts of actions, understandings of privacy, and relationships does Dropbox expect its users to maintain? Following work by feminist STS scholars and the concept of the gender script (van Oost 2003), I have argued for the use of the term 'value script' to capture how one aspect of subjectivity – privacy values – Dropbox might inscribe on its users. How are privacy values scripted into the technology – into Dropbox – and how are these values communicated and prescribed to users?

To answer these questions, I will conduct a textual analysis of Dropbox's official policies. This methodology will allow this project to draw out the multiple themes and narratives Dropbox uses to discuss privacy. In other words, what sorts of user scripts or 'value scripts' regarding privacy does Dropbox prescribe to its user. The documents I will analyze include: the terms of use, the official legal contract outlining the rights and responsibilities of both Dropbox and its users; the privacy policy, which contains information on what personal information Dropbox can or will collect, how they use it, and what users should do to protect personal information; the security terms, which outlines how Dropbox protects personal information and data; and the acceptable use policy which outlines ways in which users should or should not use the software. These documents are crucial for my purposes, as they are the only place in which Dropbox

comprehensively outlines the actions it expects of its users, as well as which actions it will undertake itself. It is thus ripe for an analysis for the sorts of user scripts communicated by Dropbox to its users. However, one minor drawback exists to using these sources to interpret user scripts: they are all carefully crafted legal documents. While they carefully lay out the expectations of users, their format and language lead their actual readership and adoption by users to be questionable. As such, Dropbox communicates much of its policies and changes to these policies through a company blog. I have included three blog posts that include the key terms 'privacy' or 'security' in the title or meta tags and communicate the company's policies and user scripts in a more informal and readable format.

This question and methodology is similar to those studied by Bodle (2011), who performs a discourse analysis of Google's privacy policies and other privacy-related discourse, and Fernback and Papacharissi (2007), who conduct a discourse analysis of the terms of agreement of numerous social media websites. Like these two articles, a critical discourse analysis will allow this project to draw out the ideal set of privacy-related actions and values, or in ANT language, the ideal user (Akrich 1992) imagined by Dropbox.

To analyze this data, I will use an adapted version of social actors approach of critical discourse analysis as outlined by Wodak and Meyer (2009). This approach looks to identify actions within the texts and to what actors and under what conditions the actions are prescribed. Thus, this method will help my project at identifying the user scripts of Dropbox. Coding is done at two levels. First, I will conduct a close reading of the data sources, identifying any actions related to privacy, security or personal data.

Second, I will further code these actions by identifying relationships with specific actors and resources required to perform this action. Each coded action will contain up to two relationships: one between the actor specified and the privacy action being discussed, and a second between the actor specified and the resources they require. Each of these relationships will be typified either as a hard/one-way relationship (actor A *must* perform action A, and/or *requires* resource Z), a soft/associative relationship (actor B *should* or is implied to perform action B, and/or *could* use resource Y), or a symmetrical relationship (there are two actors involved in the prescribed action, who are acting on each other).

These relationships will be analyzed to identify the prevalence of certain types of relationships between actors, certain types of actions prescribed to particular actors and certain types of resources assumed to be held by some actors. The prominent themes that are identified among these relationships will be extracted and analyzed in order to identify and understand Dropbox's user scripts. In particular, three prominent themes were noticed in these policies and communications from Dropbox: trust, security and privacy. All three form a significant part of the value scripts that Dropbox inscribes upon its users. Users must trust certain actors, including Dropbox, some third parties and certain technological standards. Part of this relationship of trust involves the offloading of security onto Dropbox. Dropbox makes clear that security is its responsibility; its user script involves an explicit directive for users to not be concerned with security. On the other hand, Dropbox prescribes the protection of privacy and personal information to its users. When discussing its own actions for the protection of personal data, Dropbox uses a rubric of security, however, when discussing users' actions for this same protection it is framed as privacy protection. In other words, Dropbox responsibilizes users; it expects

them to value and self-regulate their personal privacy, while at the same trusting Dropbox and associated actors to uphold a certain standard of security. Taken together, these themes reflect an important effect of Dropbox's user script: they affirm that users are to trust and to delegate certain actions to technologies, standards and non-human actors, while the source of potential error, of breakdown, of privacy infringement is human action. As such, this user script calls for a certain vigilance, constraint and self-regulation when it comes to personal information.

Trust

As discussed above in the introduction, heterogeneity necessitates trust. If Dropbox pulls together many heterogeneous actors – users, technologies, privacy policies, and so on – there must be some level of trust between these actors. As discussed above, actors build networks through translation, through aligning the interests of these heterogeneous actors; however, these interests cannot be aligned without trust, without the belief that other actors will behave in the expected way. Thus, Dropbox and its users must trust that certain programs, servers, or third parties behave as expected. Just as differentiation of social action, understood on a macro scale, requires trust in order to reduce this complexity and allow for a smooth-running social system, the differentiation, the heterogeneity of networks requires some of level of trust and predictability amongst actors to allow for the durability of the network.

This connection between trust, durability and technology is best exemplified using Bruno Latour's (1992) example of the door closer. Latour (1992) traces a hypothetical history of the door, from a simple hole in a wall to a modern door with an automated closing mechanism. Each step along the way involves some form of

delegating or shifting an action to a new human or non-human actant, from shifting the act of tearing and rebuilding a hole in a wall to a set of hinges and slab of wood, to delegating the act of closing a door behind us to grooms and eventually automated door closers. As we delegate these actions, shift them to new actors, we essentially create a system of interdependency; we trust that the groom will do his job and we trust that the automated door closer will work. If they do not work, further actors must be incorporated: if the groom does not perform his job, new actors must be incorporated to discipline the groom, while if the automated door closer breaks down technicians are called for repairs (Latour 1992). We treat the automated door closer as a black box; we do not question its internal workings, but trust that it will work. If it breakdowns, we do not revert back to the hypothetical stage of tearing a hole in the wall or closing a door ourselves, we further delegate action to other actors. As the complexity of the apparatus grows, as further heterogeneous elements are drawn together, trust serves as mechanism to reduce the heterogeneity. In order to not have to undertake the onerous process of breaking through a wall every time we want to enter a building, we must delegate action to humans and non-humans and trust that they will perform accordingly.

In sum, this imagined history of the door shows how a simple technological artefact involves a complex process of delegated action. The effect of this delegated action, however, is the reduction of heterogeneity. By delegating action to new actors, technologies become black-boxed; we no longer have to perform every action ourselves, to know the workings of every minute step in the process of entering a building, but can rather depend and trust certain artefacts. As a result, we do not see a door as a complex task comprised of many heterogeneous elements; we see it simply as a door, as a means

to enter a building. The heterogeneity of the door closer is reduced through entrusting other actors. Thus, to repeat what was mentioned above: heterogeneity necessitates trust. As actor-network theory looks at how heterogeneous elements are drawn together as well as how this heterogeneity is reduced, trust becomes an important mechanism in the latter.

What is noteworthy about trust in the case of Dropbox, however, is that trust does not become an implicit side effect of the building of a heterogeneous network and the reduction of complexity; it becomes an explicit element of the user scripts of the technology. Dropbox delegates much action to other actors – users, third parties and technological standards – and as such must trust these actors to behave accordingly. However, trust is also a mechanism by which Dropbox enrols users. It is not sufficient for users to simply trust the technology to which they delegate the action of file storage. Dropbox explicitly lays out which actors are to be trusted and how users should trust these various actors. Such an explicit direction to trust seems to be the norm when it comes to cloud computing services and their official policies and terms. For instance, when analyzing Google's privacy policies and concludes that "users are persuaded to *trust* in the transparency of Google's intentions" (Bodle 2011: 157, my emphasis). Fernback and Papacharissi (2007) go a bit further by claiming that many discursive elements found in privacy policies – both implicit and explicit – serve to foster trust in web service providers without giving any real assurances of privacy protection. With a lack of oversight agencies or international regulation, trust becomes the primary means of ensuring user privacy (Bodle 2011), although often privacy is still at risk despite the efforts of the company to build that trust (Fernback and Papacharissi 2007).

In a similar fashion, Dropbox makes a great effort to communicate its trustworthiness to its users. For instance, Dropbox leads off a blog post regarding updates to its privacy and security policies with the follow: "Everyone who works at Dropbox knows our most important asset is the trust of our users" (Dropbox April 21, 2011). Similar to as in Bodle's (2011) study of Google, trust and transparency are closely intertwined in Dropbox's communications: changes were made to official policies "to be more user friendly and transparent" (Dropbox April 21, 2011). For the most part, Dropbox implies that users trust them. Nowhere do they directly say 'thou shalt trust us', but rather use softer language. Often this is used to establish trustworthiness by using a conversational tone: "the last thing we want is to let you down" (Dropbox April 21, 2011). Other times it used to imply that users already trust Dropbox and they do not need to further establish trust, only reaffirm it: "the trust placed in us by millions of people to keep their valuable data safe" (Dropbox July 1, 2011) and "we are proud of the trust placed in us" (Dropbox N.d.a). At other points, a two-way trusting relationship is established. For example, while Dropbox assumes users have placed trust in them, they hope to make this a reciprocal relationship: "in exchange, we trust you to use our services responsibly" (Dropbox N.d.a). While there is no firm direction that trusting Dropbox is a must, it is clear that their user scripts involve an element of trust. Users are not told to trust Dropbox in order to use the service, but are rather persuaded in a way similar to Google's privacy policies (Bodle 2011).

One way in particular in which this relationship of trust between Dropbox and its users is fostered is through the treatment of data ownership. Data ownership is a contentious issue in the use of, as well as the regulation of cloud computing software

(Bianco 2009; Jaegar et al. 2009; Office of the Privacy Commissioner of Canada 2011). Dropbox's efforts to communicate its trustworthiness involve an explicit stance on this issue: users keep ownership of their data. This point is made explicit almost immediately in Dropbox's Terms of Agreement: "You retain full ownership to your stuff. We don't claim any ownership to any of it" (Dropbox March 26, 2012). Much of Dropbox's official communication relates to how they retain user data and information, as that is the essence of their service. A whole section of the Privacy Policy is dedicated to 'data retention', outlining how the company retains data as long as an account is active and potentially longer if legally required (Dropbox April 10, 2013). Nevertheless, by carefully avoiding claiming ownership of user data, Dropbox is able to maintain its aura of trustworthiness. Subtly building this relationship of trust allows them to communicate trust as an integral part of their user scripts. Carefully crafting their trustworthiness implies that users must trust Dropbox in order to use the service.

Apart from inscribing trust in itself onto its users, Dropbox also directs certain third parties which users should trust. These other actors are referred to in Dropbox's official communications as "trusted third parties we work with to provide the Services" (Dropbox March 26, 2012). The most commonly cited trusted third party is Amazon, to whom Dropbox outsources certain security and storage processes. Dropbox makes it clear that they trust these third parties; they delegate action to other actors as they build their network which as we have seen, involves a certain level of trust and black-boxing these new actors. This trust is passed onto users. Users delegate action (file storage and security) to Dropbox, who delegates certain actions to third parties. As such, in the relationship between Dropbox and users, the trustworthiness of third parties is extended

from Dropbox to users. This is done through Dropbox's user scripts, through its official communications and its efforts to enrol its ideal user.

When passing this trust onto users, however, Dropbox does give users the option to open these black-boxes. Take the following example: "we use Amazon's S3 storage service to store some of your information (for example, your Files). You can find more information on Amazon's data security from the S3 site" (Dropbox April 10, 2013). Here, Dropbox continues to entrust and delegate action to a third party. This trust is implicitly passed on to users as Dropbox enrols them. Nevertheless, the possibility is there that users do not want to entrust Amazon's S3 storage service. In such situations, it is their responsibility as prescribed by Dropbox to learn what this third party does. While this might seem to undermine the relationship of trust Dropbox carefully builds, I would argue it plays an alternative role. It functions to responsibilize the user, something that will be discussed in more detail below. This responsibilization is made most clear when discussing other third parties: "you should make sure you trust the application and that it has a privacy policy acceptable to you" (Dropbox April 10, 2013). Rather than provide an opportunity for distrust, these user script display Dropbox's trust for certain third parties. They pass this trust onto to users through association; if you trust us, you trust whom we trust and we do not need to question their internal workings. If users want to build a relationship of trust directly with these third parties, it is their responsibility to learn how the third parties work – to open up these black boxes.

This process of delegating trust to other actors and passing this trust onto users is also evident by how Dropbox employs technical standards in its user scripts and official communication. Their official communications and policies make numerous references

to technical standards and certification, such as the U.S. - E.U. and U.S. – Swiss Safe Harbour frameworks (Dropbox April 10, 2013), the AES-256 standard (Dropbox N.d.b) and most notably, the TRUSTe Privacy Seal (Dropbox April 10, 2013). These standards and certification serve the primary purpose of building Dropbox's trustworthiness; to show that they are legitimate in the eyes of regulatory frameworks, technical standards and impartial industry regulators. The latter of these is the most important. As discussed by Fernback and Papacharissi (2007), the TRUSTe Privacy Seal is often shown in web companies' official policies as a way to build the trust of its users. Not only is the name of the certification telling, but so its purpose: if this company is trusted by an organization of impartial experts, it can be trusted by individual users.

However, there is a secondary layer of trust at play by referring to these standards. Dropbox's user scripts require users to trust these standards themselves. Technical standards are the quintessential black-box. Take the simple example of the yard: when something is measured, we do not need to question what a yard is, how it came to be defined, the physical object it originally referred to or the scientific processes in the laboratories in which this original object is replicated.[11] We simply trust that our given yard stick is in fact one yard. All the historical and scientific heterogeneity is reduced to a taken-for-granted standard metrology. Similarly, when Dropbox claims it adheres to the AES-256 standard of security or is recognized by TRUSTe, these technical standards are taken-for-granted. Users are not expected to understand the intricacies of the AES-256 standard or the internal policies used to decide whether a given company gets a Privacy Seal by the folks at TRUSTe. Users are not expected to open these black boxes.

[11] This example of the yard, its history and its reduction to a black-boxed standard is borrowed from Barry (2001).

Rather, the user script communicated by Dropbox involves an expectation of trusting the reliability, validity and authority of these technical regulations, standards and certifications.

Security

The nexus between reliability and black-boxes can be further understood when looking at the second theme observed in Dropbox's user scripts: security. Dropbox further establishes its reliability and trustworthiness by continually reinforcing that it will handle security; that it has the technical resources and expertise to keep users' data secure. For example, Dropbox highlights its responsibility, objective and expertise when it comes to security in its privacy policy: "The security of your information is important to us. When you enter sensitive information (such as a credit card number) on our order forms, we encrypt the transmission of that information using secure socket layer technology (SSL)" (Dropbox April 10, 2013). These technical resources and expert knowledges are not explained in the depth – these black-boxes are not opened – but are nevertheless utilized by Dropbox to firmly establish data that security is its domain and expertise. For instance, in a blog post explaining updated security measures, Dropbox leads by stating "security is a responsibility we take very seriously and a topic we want users to understand" (Dropbox July 1, 2011). Dropbox wants to communicate its expertise on security to its users. In doing so, it can said that Dropbox becomes an "obligatory point of passage" (Callon 1986) for data security. Since users do not have the knowledge, expertise or resources for this high level of data security, they must trust Dropbox and act according to their user scripts in order to achieve this security. They are obligated to pass through Dropbox.

There is one exception to this trend noticed in Dropbox's official communications. In a blog post, Dropbox states:

> "Dropbox manages encryption keys for you. The reason is many of the most popular Dropbox features — like accessing your files from the website, creating file previews, and sharing files with other people — would either be impossible or would be much more cumbersome for users without this capability. But we're also ok if you want to manage your own encryption by using products like TrueCrypt with Dropbox" (Dropbox July 1, 2011).

In this short excerpt, Dropbox achieves three things. First, it reinforces that it handles security for its users because it is "cumbersome for users without this capability" (i.e. for users who do not have Dropbox's technical expertise). Second, it cedes that some users might have this expertise and wish to take security and encryption into their own hands. Lastly, it reinforces that security is a technical matter that requires technical resources (i.e. TrueCrypt) for those with the expertise to know where to acquire them.

Nevertheless, for the most part, users are assumed to have the expertise and resources for data security. In fact, users are rarely mentioned when security is being discussed. When the relationship between users and security is discussed, it is typically in a negative sense. Users are instructed not to question or test the security of Dropbox's systems. For example, much of the acceptable use policy involves firm directives to users to not attempt to breach the security measures put in place by Dropbox: "you must not, and must not attempt to, use the services to do the following things… probe, scan, or test the vulnerability of any system or network; breach or otherwise circumvent any security or authentication measures" (Dropbox N.d.a). This policy makes clear that Dropbox should be trusted with security and users should not attempt to tamper with their technical expertise and resources – they should not open the black box (Woolgar 1991).

When Dropbox discusses security, they remove much, if not all, of the human element involved in protecting a secure network. For example, Dropbox employs "technical access controls that prohibit employee access except in [sic] rare circumstances [i.e. when legally required]" (Dropbox April 21, 2011). They delegate most action to technological artefacts and processes, making clear that this is a technical matter that requires an objective, technical knowledge to understand. not only is security delegated to the black-boxed AES-256 standard discussed above, but most of the security processes and controls outlined by Dropbox in their official communications are shrouded in technical language and jargon: "Your files are sent between Dropbox's desktop clients and our servers over a secure channel using 256-bit SSL (Secure Sockets Layer) encryption, the standard for secure Internet network connections" (Dropbox N.d.b); "Two-step verification is one of several steps that we're taking to enhance the security of your Dropbox" (Dropbox August 27, 2012); and "Amazon and Dropbox also employ significant protection against network security issues such as Distributed Denial of Service (DDoS) attacks, Man in the Middle (MITM) attacks, and packet sniffing" (Dropbox N.d.b). Each time Dropbox explains how secure its system is or how its security works, it delegates data security to black-boxed technical processes, of which it has the necessary expertise and resources to maintain and protect.

By framing security as a purely technological issue, Dropbox reaffirms its trustworthiness by appealing to the reliability of black-boxed objective technologies. Each of these technological processes and standards that are in place to keep users' data secure are seen as reliable; as we have seen above, when delegating action to a black-boxed technology, we essentially entrust that actant to behave accordingly. One

exception to this trend was observed; in a blog post, Dropbox acknowledged that there was a technical bug that compromised security (Dropbox June 20, 2011). Nevertheless, this is the exception and not the norm; Dropbox quickly re-establishes the reliability, trustworthiness and objectivity of its technological resources. This implies that if personal information is compromised, it is an issue with the human elements in this technology (Bodle 2011). However, since Dropbox makes clear that its employees do not have access to user accounts and black-boxes the security processes and standards, the only human element remaining is users themselves. Thus, although Dropbox makes clear that it will handle security and that users can trust them with protecting data due to its technological expertise and resources, it essentially responsibilizes the user for protecting his or her own sensitive information. Security is an objective technological issue that requires technical resources and expertise. Privacy protection is a subjective human issue that requires self-regulation and vigilance. This responsibilization of the user is a vital part of Dropbox's user scripts and is the topic of the following section.

Privacy

The fact that Internet companies offload responsibility for privacy protection onto users themselves is not a novel idea. As mentioned above, Bodle (2011) discusses the same process in relation to Google's cloud computing services. Google's privacy material responsibilizes the user through three interrelated linguistic mechanisms: modality, or the use of vague signifying language such as 'may' or 'might'; lexical enhancements, or the use language that places collection of data together with user enhancement and improved services; and coherence, referring to the internal consistency of these documents and the use of lexical choices and modality together (Bodle 2011).

Additionally, Bodle (2011) discusses how users are further responsibilized through directives to cross-check Google's various policies; Google does not make clear the internal consistency between their general policies and policies for specific products, but offloads the responsibility to users to ensure that they understand all policies that affect their use. The effect of these mechanisms is to obscure the extent to which Google collects personal data (Bodle 2011), which ultimately frames privacy (here understood as the absence of collecting personal data) as the antithesis to convenience and user enhancement. This dichotomy or trade-off is presented as a choice for users, as free consumers, to make (Fernback and Papacharissi 2007).

My findings in analyzing Dropbox's privacy material are similar, though with some differences. For instance, I found that the extent to which Dropbox collects data was not as obscured as Bodle (2011) finds with Google. When outlining its responsibilities and actions for collecting user data, Dropbox typically uses hard language: "we collect some personal information" and "we automatically record information from your Device, its software, and your activity using the Services (Dropbox April 10, 2013). That being said, there are several uses of vague language when discussing personal data (e.g. "we may collect and store the following information" or "we may collect personal information that can be used to contact or identify you" (Dropbox April 10, 2013)), though it is not the primary mechanism by which this is communicated. Often, these clear statements on Dropbox's data collection practices are flipped so that the user becomes the subject: "you consent to the collection, transfer, processing, storage, disclosure and other uses described in this Privacy Policy" (Dropbox April 10, 2013). Here, Dropbox accomplishes two things. First, it makes clear that

collection of personal data is a given; it is not framed as something that may or might happen, but as something that will happen, and is treated as a self-evident, taken-for-granted fact. Second, Dropbox communicates a central tenet of its user scripts: users *must* consent to this data collection. The way the above statement is framed suggests not only that Dropbox reaffirms the choice between privacy and convenience, but also that it assumes and expects users to have already made this choice in favour of the latter. A key value script it communicates is that users should value convenience over privacy, of use of the service over the absence of personal data collection.

A glaring similarity between Dropbox's privacy material and that of Google outlined by Bodle (2011) is the use of language of enhancement alongside discussions of data collection. For example, the language of 'improving services' and 'better understanding' user needs is frequently employed: "we also use "cookies" to collect information and *improve our Services*"; "We may use 'session ID cookies'… *to better understand* how you interact with the Service"; "personal Information is or may be used: (i) to provide and *improve our Service*… (iii) *to better understand* your needs and interests" (Dropbox April 10, 2013, all emphases are my own). This language is also central to Dropbox's less formal communications found in its blog: "information about how people use Dropbox is really important to helping us build a better product" (Dropbox July 1, 2011). These sorts of statements are common in Dropbox's communications and serve to reinforce the trade-off between use and privacy. They associate the collection of data with enhancements for the user and by extension thus associate privacy and a lack of collection of data with the status-quo and no user enhancement. Thus enhancement, use and convenience become the antithesis to privacy

in Dropbox's user scripts: a dichotomy that is implicitly framed as a choice that users are expected to make.

Another interesting mechanism by which Dropbox offloads privacy is by framing its data collection practices as a necessity. It can be argued that by associating data collection with user enhancement, Dropbox frames the former as a necessity (we need to collect data in order to give users what they really want and need); however, this necessity of data collection is made most clear in relation to how Dropbox discusses data retention and disclosure and how it communicates its legal obligations. At several points, Dropbox makes reference to the fact that it must keep and occasionally disclose user data for legal purposes, most notably in its Privacy Policy:

> "We may disclose to parties outside Dropbox files stored in your Dropbox and information about you that we collect when we have a good faith belief that disclosure is reasonably necessary to (a) comply with a law, regulation or compulsory legal request; (b) protect the safety of any person from death or serious bodily injury; (c) prevent fraud or abuse of Dropbox or its users; or (d) to protect Dropbox's property rights" (Dropbox April 10, 2013).

Dropbox further states that it "may retain and use your information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements" (Dropbox April 10, 2013). Thus, while users are given (and must make) a choice between privacy and convenience, Dropbox is incapable of making such a choice: it must collect, retain and disclose certain personal information in order to improve its services and satisfy its legal obligations. As discussed above in relation to security and trust, Dropbox is framed as an impartial, technical actor. The realm of human action and choice, and hence the responsibility for choosing to protect one's privacy, falls onto users.

This responsibility of the user to protect his or her own privacy is best captured in the following statement from Dropbox's Terms of Agreement: "You, and not Dropbox, are responsible for maintaining and protecting all of your stuff" (Dropbox March 26, 2012). This idea is reinforced through several actions and behaviours prescribed to users throughout Dropbox's official communications. For instance, the Privacy Policy contains the following instructions: "You can instruct your browser… to stop accepting cookies or to prompt you before accepting a cookie from the websites you visit"; "If you do not wish to share files embedded with your geo-location information with us, please do not upload them" and "If you don't want to store location data in your photos or videos, please consult the documentation for your camera to turn off that feature" (Dropbox April 10, 2013). Each of these instructions involves some sort of data collection practice as well as instructions for how users can opt-out of this specific practice if they happen to choose the privacy side of the privacy/convenience trade-off. Each one also implies that users know how to perform the given action; users know how to turn off cookies in their browser or work the settings of their camera. It is the user's responsibility to protect their data should they not want it shared.

In sum, Dropbox offloads the responsibility for protecting privacy and onto users themselves. Their user scripts prescribe a set of actions that users must take in order to control which personal data gets collected and what gets kept private. Dropbox imagines its ideal user as someone who values privacy over convenience, but ultimately as a free consumer who must make the choice between these two poles. This idea of responsibilizing the free consumer to make a choice about his or her own well-being is consistent with the ideal subject or citizen of neo-liberalism. For instance, Rose (1999)

discusses how 'advanced liberal' modes of government involve strategies and techniques that serve to instill a sense of responsibility, vigilance and self-regulation in citizens. Much of this responsibility involves making choices in a free market. Thus, Dropbox's user scripts that involves users making choices and self-regulating their privacy is consistent with this mode of government. The expectation that users be responsible and vigilant when it comes to protecting their personal data fits in with a regulatory framework based on principles of deregulation, autonomy of consumer citizens and "faith in the 'good practice' of industry"(Bodle 2011: 159), or alternatively, a framework based on "governing at a distance" (Rose 1999).

Conclusion

Responsibility and self-regulation of one's personal data and privacy is the central tenet of Dropbox's user scripts. Users are expected to value convenience over privacy and control what personal data can be collected. However, as we have seen, this is not the only important theme that is observed in Dropbox's official policies and communications. Dropbox also expects its users' trust as well as for users to trust certain third parties and technical standards. It outlines how it has the expertise and resources to secure user data. However, when it comes to privacy protection (not security) and controlling what data gets collected, it is expected that users take control.

I argue that what connects these themes is the distinction between Dropbox as a technical entity and users as human. While this distinction may seem self-evident, the way it is communicated by Dropbox has important effects. Namely, it presents Dropbox as an assemblage involving technological resources, expertise and standards. Dropbox and the other actors and third parties it partners with are thus presented as black-boxes:

closed entities that are durable, objective and trustworthy. Users, on the other hand, are simply human, subjective and prone to error. Therefore, personal privacy being unnecessarily put at risk is the responsibility of users as human actors. As such, self-responsibility and control for protecting personal data and privacy become the central expectation for Dropbox's ideal user. However, what happens when this trustworthy technology fails? What happens when Dropbox mistakenly puts user data at risk? What happens when the black-box breaks down? These sorts of concerns, and the reactions of users in situations when the taken-for-granted trust and privacy are put into question, will be explored in the following chapter.

5 When Trust Fails: De-Scription, Margins and Breakdown

Simply looking at the user scripts of a given technology, such as Dropbox, falls dangerously close to the technological determinist assumptions I wish to avoid. One must also look at the reverse and "go back and forth continually between the designer and the user, between the designer's projected user and the real user" (Akrich 1992: 208-209, my emphasis). As discussed in the previous chapter, for the purposes of this project the projected user is the user imagined and assumed in Dropbox's official policies and user agreements. To observe the real users of Dropbox, I turn to Dropbox's Community Support forums. The use of these user forums as a data source is done for two reasons: one, it seems fitting to employ an Internet-based methodology for studying an Internet-based technology, and more importantly, two, these user forums provide discussions on privacy, trust, and cloud computing that are rich in qualitative data. Since help forums are a readily available option for users, this methodology provides many diverse voices and understandings of privacy. However, it also leads to one small limitation: it means my definition of users must be narrowed to include only those users who participate in forum discussions and not those who might be casual or less-invested users. Nevertheless, this limited definition of user is accepted for the purposes of this project and to keep its scope narrow.

These forums present a good case for studying the de-scription of Dropbox's privacy scripts for two reasons. One, they present textual representations of users' understandings of Dropbox, its use and practicality, its privacy and security concerns, and the applicable laws and regulations. It provides these representations in an unfettered form, that is, free from certain research biases such as the Hawthorne effect. Two, the

forums are designed to discuss issues or problems with Dropbox and how to resolve them. Thus, the forum posts represent the most elementary form of technical breakdown: when the inside of a technology (i.e. its inner workings and assumed uses) do not match up with the outside (i.e. its actual use or performance) (Akrich 1992: 207). It is in these sorts of situations that the de-scription of technical objects becomes observable; there is a back and forth, a communication, a process of co-production between the technical and the social (Akrich 1992; Jasanoff 2004).

I will analyze all threads that have 'privacy' in the title or first post of a thread over the past 3 years. This time frame is useful as it will cover the time in which Dropbox suffered its privacy 'fiascos', discussed above, but will be short enough to keep this project's scope limited. Through this analysis of forum posts, I will be looking to identify users' concerns, understandings and actions regarding the protection of personal data and privacy. These will be read against the prescribed, ideal uses discussed in Chapter Four to explore how users might accept, reject or negotiate 'value scripts'.

In order to juxtapose the user scripts offered by Dropbox to the de-scription efforts of users, I will use a similar data analysis strategy as in Chapter Four. I search the text for actions and the relationship between a given action and who it is prescribed to and under what conditions. Which actions do users expect Dropbox to perform? What do they see as being their responsibility as users? When Dropbox employees respond, do they provide a different understanding of user rights and responsibilities? I explore these sorts of questions, with one additional layer of analysis: I differentiate between the original post in a given thread on the forum (the problem) and the various responses (the solution(s)). What sorts of problems are communicated by users? What sorts of action

do they think should be taken by themselves or Dropbox to resolve these problems? How do other users respond? What kinds of actions are involved in their solutions? Who should these actions be prescribed to? My responses to these questions always keep the findings of Chapter Three in mind; that is, the sorts of problems and solutions users come up with when using Dropbox is read in conjunction with the imagined and assumed user communicated by Dropbox, one that trusts the security and technology of Dropbox and takes any other privacy matters into their own hands. In other words, I attempt to read the representations of real users in relation to the designer's projected user; I go back and forth between outside and inside the technological object.

Essentially, this chapter engages with Akrich's (1992) concept of description and Star's (1991) critique of ANT. By looking at Dropbox's community support forums, this chapter analyzes textual representations of users' concerns and issues regarding privacy. If users express concerns on these forums, it is assumed that something has gone wrong, either with the black boxed technology, or the user's acceptance of the prescribed use of the technology. They are at a 'zero point' in which they do not fit comfortably as the 'ideal users' imagined by Dropbox but are instead involved in descripting their own privacy scripts, perhaps pulling from understandings of privacy from other socio-technical networks. Thus, these texts represent the moment of action – when users actually use Dropbox – and how they might negotiate the privacy-related 'value scripts'.

In exploring these sorts of questions, three themes become noticeable. First, the solutions provided by users largely conform to Dropbox's ideal user. Their solutions are predominately framed in the language of trust and self-regulation. This is evidence of some level of stability, of closure of Dropbox, as its users are mostly standard and in-line

with the user assumed by the company. However, keeping in mind Star's (1991) critique of actor-network theory discussed in Chapter Two, we must be aware of the margins when standard uses exist. This is the second observation of this chapter; the problems presented by new forum threads can largely be understood using a framework of marginal users. These users have varying levels of trust in Dropbox and varying abilities to self-regulate and protect their own privacy. The solutions provided to these users typically involve an attempt to communicate trust and expertise in order to 'get the user on board'. There exists an interesting tension in which the marginal users attempt to maintain their marginality as long as possible (Star 1991), for example by refusing to trust Dropbox, and the attempts of other standard users and Dropbox employees to reduce this marginality, to further stabilize the boundary between user and non-user.

The last, and perhaps most important, theme involves technical breakdowns, namely situations in which Dropbox suffers a technical bug or is named as a potential contributor to the NSA PRISM surveillance program. It is in these situations, that the stability of Dropbox comes into question; the users that conform to Dropbox's ideal user are now in the minority and the trust that is the central part of this ideal user becomes shrouded in doubt. Users respond to these breakdowns in varying ways – some quit Dropbox, some seek answers from employees, some suggest new actions Dropbox should undertake to protect user privacy – however one commonality is always present: when trust disappears, privacy appears. When users feel that they cannot trust Dropbox's perceived objectivity and technical expertise, privacy becomes negotiable and contested.

Conformity and Stabilization

For the most part, users – particularly those who are responding in forum threads, who are providing the solutions – conform to Dropbox's ideal user. These users accept and perform the two actions prescribed to them: trust (in Dropbox's security) and privacy protection. For instance, one of the longer threads on the forum was in response to one of Dropbox's blog posts outlining changes to their privacy policy and terms; most user responses seem to reaffirm users' trust in Dropbox. David S. writes "in my experience, Dropbox is one of the most open and transparent companies I've seen" (item 13, page 1)[12]. Similar sentiments (as well as some opposing sentiments discussed below) are common in this thread; users' trust in Dropbox is rooted in communication and transparency between users and the company. Furthermore, in a thread about implementing Dropbox in a workplace environment, Richard P. writes: "You and I both know that I am a Dropbox supporter" (item 10). Despite problems with setting up the software in his workplace, this user's trust in Dropbox never wavers; it is the constant basis upon which possible solutions are explored.

In agreement with Dropbox's user scripts, his trust in Dropbox is due to its technical resources and expertise for keeping data secure. For example, in response to a user concern about the security of data stored in the Dropbox folder on their PC, Wes P. replies: "At some point we have to decide if the company is reputable, look at their track record in protecting our files, and decide whether we trust them. 60 million people so far trust Dropbox, and haven't been taken advantage of. I think we're in good hands" (item 42). In a similar but perhaps more telling example, Andrew W. starts a thread by saying

[12] "Items" refer to the individual forum threads. For a complete list of the threads analyzed in this chapter with some bibliographic information, refer to Appendix A.

"No matter what happens with the security things going on, I will continue to use Dropbox because it is awesome" (item 30). In both situations, as well as several others, users express an undoubtable trust and reverence for Dropbox; they do not question things like security because Dropbox is the reliable technical expert that takes care of this domain.

Although users mostly trust Dropbox with security, they still acknowledge that private information is at risk. At times this might lead to a distrust in Dropbox as the party with control over one's data, for the most part it does not; users almost exclusively conform to Dropbox's ideal user and self-govern privacy protection and make all attempts to mitigate the risk of disclosure of personal information themselves. For example, a common solution that is provided to various real or perceived problems is encryption. As discussed in Chapter Four, Dropbox recommends that its user use a third party application to encrypt their files themselves in order to protect their sensitive information. Users act largely in concordance with this recommendation. From questions as varied as 'Can Dropbox access my stored data' (item 5) to 'how secure are shared folders' (item 28) and 'where are Dropbox servers located' (item 68), a common solution provided in response is for users to mitigate any concerns by taking privacy protection into their own hands and using encryption software to protect their data.

However, there are other ways in which users conform to Dropbox's user scripts by agreeing to take control of their own privacy protection. For instance, in one thread in which a user is asking how to improve the privacy of shared but sensitive data, another user responds with the following solution: "I would suggest you do not share those sensitive data at all" (item 1). This user is advised to protect his or her own privacy as

well as the privacy of others by taking responsibility over what data is given to Dropbox. In another thread, a user expresses concerns over personal privacy after buying a premium Dropbox account over eBay; other users' solutions are not directly related to the security and privacy concerns raised, but rather about the responsibility of the original user to know the applicable laws and regulations surrounding such a situation. This is perhaps best summarized by Kevin L.: "You should have done your research properly before parting with your money" (item 4). Protecting privacy is not something that is assigned to Dropbox, but something that is the responsibility of the user; in this case that responsibility involves researching the laws that apply to personal privacy and the transfer of information and information technology.

Thus, it can be seen how users often conform to the user scripts discussed in Chapter Four by trusting Dropbox and taking responsibility for protecting one's own private information and material. There is a certain level of consistency between Dropbox's ideal user and the actual user. This is evidence of some level of stability, of closure of Dropbox as a technological entity. This is not surprising, as it has been a product on the market for several years, moving far beyond its design and beta stages. Nevertheless, this reduction of difference between the imagined and actual users is important in understanding the de-scription of a technological entity. Akrich (1992) argues that technologies and designers not only delegate certain competencies and responsibilities to certain actants, but as the disparities between ideal and actual use become reduced, these user scripts become naturalized. As a technology becomes stable, durable or 'natural', users cease to question certain ways of behaving. As Akrich (Akrich 1992: 207) importantly points out, this does not just mean that use of the given

technology is being taken for granted, but that these user scripts may "lead to new arrangements of people and things… [and] new forms of knowledge about the world." The level of stability in my observations of Dropbox could be an example of such a phenomenon; users cease to question certain ways of thinking about privacy. They start to adopt a certain privacy script: that privacy is something that can be delegated to technological objects, presuming one can trust the objectivity of said object, and any subjective decisions that need to be made regarding privacy protection are the full responsibility of individuals.

Distrust and lack of expertise: the marginal users

The unquestioned adoption of Dropbox's privacy scripts is not universal, however. As Star (1991) reminds us, simply looking at standard uses of a given technology ignores the multiplicity of users; it ignores the fact that marginal users exist – users that 'slip between the cracks' and do not fit perfectly with predetermined actions, behaviours and categories. This idea was evident when examining Dropbox's user forums. While most users adopt Dropbox's privacy scripts, several users do not adopt this standard use; they remain marginal. There are two ways in which users do not necessarily line up with Dropbox's ideal user. First, they do not bestow Dropbox or its associated third parties with the appropriate level of trust. Second, they do not have the expertise or knowledge to self-regulate privacy. In both situations, other users providing solutions attempt to further reintegrate these marginal users. They attempt to prove the trustworthiness of Dropbox or teach users how they can regulate their own privacy. In other words, they are involved in further standardizing the actions, beliefs and privacy values of Dropbox users.

In several forum threads, hints of distrust can be seen in the problem presented by the original poster. For example, some users express doubt about Dropbox being able to access their stored files (items 5, 17, 21, 27). This distrust is often levelled at Dropbox employees and not necessarily the technological entity itself. John J., after admitting he is a new Dropbox user, states "[I've] read [a lot] about the employees [that] can open and read our files" (item 27). Bruce M. writes: "I heard recently that Dropbox employees can see the files in my Dropbox folders" (item 5). Other users are not as explicit in naming Dropbox employees as the target of their distrust: a user simply named 'a' recalls: "I moved my private files out of Dropbox and stopped paying for extra storage because Dropbox wants to have access to content of my files.... For some reason..." (item 46). Similarly, Andrew M. asks "what scanning do Dropbox do of the files in your account for copyright or other restricted material?" (item 21). What all these users have in common is varying levels of trust in Dropbox and its employees for respecting and protecting their personal data.

This distrust also extends to certain third parties. As discussed in Chapter Three, Dropbox's user scripts require not only that users trust the company and the cloud technology, but also that they trust certain reputable third parties. However, some users, while trusting Dropbox, have difficulty in extending this trust to third parties. This is perhaps best exemplified by user 'a' whom, in a discussion of a third party application that should be trusted to work in conjunction with Dropbox, sarcastically remarks:

> Right. I trust DropBox, a third party with my private files, it keeps password encryption, and now they offer me to use a fourth party. But I think I am paranoid here. Ralph Holzmann, who created Sendtodropbox seems like a nice guy. He also promises he does not keep files of DropBox users who want to use email to save their personal files to DropBox. Silly me. (item 23)

Like users who have varying level of trust in Dropbox and its employees, this shows varying levels of trust in associated third parties. They do not accept or take for granted the user scripts and trustworthiness of Dropbox. Consistent with Star's (1991) discussion of standards and marginality, we can see how not all users are the same; they each have their own multiple affiliations and interact with the standard uses and privacy scripts of Dropbox in their own way. In other words, they are marginal users who do not line up perfectly with the ideal standard user imagined by the company.

Users not conforming to the standard ideal user imagined by Dropbox can also be noticed in the varying levels of knowledge as to how one should regulate their own privacy. For example, many users want to password protect the Dropbox folder on their personal computer, only to have other users explain that this is impossible and one should simply password protect the user account on the computer (items 2, 3, 7, 65). As should be expected, several of the problems presented on a help forum step from users not having the knowledge, but having the desire, to ensure their data is sufficiently protected. This lack of knowledge can be seen by such thread titles as 'help me understand this security please' (item 25) and 'Don't even know what to call it' (item 14), both of which involve a user with an issue regarding regulating their privacy but reaching out to other users to help them. It is interesting to note that none of these users question that they should be the own regulating their privacy. This is further evidence of a standard use but users that do not necessarily fit with this predetermined vision of the user but rather interact with this standard category in multiple ways.

In these situations in which users do not conform to the ideal user but rather question certain central tenets to Dropbox's user scripts, there is a noticeable effort to

reintegrate these users. In situations when users display varying levels of trust or knowledge, there is a clear communication of trust and expertise to further enable these users to conform to Dropbox's user scripts. For instance, when users display varying levels of trust, other users make concerted attempts to highlight Dropbox's trustworthiness and reliably; this is often done in a similar manner to Dropbox's official communications by focusing on the company's objectivity, security and adherence to technical standards and regulations. In response to worries about employee's accessing personal data, Chen S. reaffirms Dropbox's objectivity, or the fact that it adheres to objective policies to protect against the subjective decisions of employees: "They can technically access everything in everyone's accounts. That is to say, the technology makes them capable of doing so. But like all sane companies, they have policies in place to describe when employees are and are not allowed to access your stuff, and to what extent" (item 6, emphasis in original).

Further reaffirming the reliability of Dropbox by showing its security measures adhering to technical standards, Xavier W. writes "Dropbox uses 256-bit encryption of your files, which is sufficient for most purposes" (item 5). Similarly, Chris J. remarks "The security is there folks, unless the law requires them to revoke the security to reveal what the law requires. It is the same for all services when it comes to what the law requires" (item 17). Dropbox is seen as an objective entity that keeps data secure in accordance with the law. This is meant to reaffirm Dropbox's trustworthiness and reliability; after discussing various 'controls' such as these legal mechanism and security standards, Bill R. bluntly states "You either believe that these kinds of controls work, or stay the heck off the internet" (item 17). In other words, unless one can trust the

objectivity of standards and of Dropbox, they should not use the service. If they do not conform to the standard user they should not be a user.

This communication of trust is also extended to third parties. For instance, in the thread discussed above when one user did not want to trust a third party application, other users continually attempt to reaffirm the reliability of this application. For example, Tom H. responds with:

> It always comes down to whom you trust. [By the way,] for the record, I have been seeing lots of tweets about him making changes and so forth to the service. Like better backend equipment etc… Ralph Holzmann from what I remember was one of the first to offer a service and he has been around for a long time. If he was going to do something bad it would have in all [likelihood] came to light by now. (item 23)

It can be seen how this user attempts to confirm and speak for the trustworthiness of this third party application and its creator in numerous ways: from stressing the time and reliable track record it holds to stressing the constant technological improvements, the 'backend equipment', that is intended to prove this applications durability, security and reliability.

Reintegrating users into the fold also takes the form of educating them in the correct ways to self-govern and protect one's own privacy. As discussed above, this often manifests itself through users providing instructions for using encryption software as a solution to real or perceived privacy threats. Here, the marginal users, the ones who do not conform to the standard user outlined by Dropbox's user scripts, are marginal because of a lack of knowledge; however, they are reintegrated into these standard uses by other users. These users communicating the solutions, once again resemble the official communications of Dropbox; they act as the objective experts that have the knowledge of security principles and reliable technologies. Often this user expertise is

extremely technical and full of jargon; for example, in response to an inquiry about deleting recently viewed files log, Richard P. writes: “He's using mismatched quotes, so you either need to use single quotes in the sql statement or escape them: sqlite3 ~/.dropbox/config.db "REPLACE INTO config (key,value) VALUES ('recently_changed3',")"” (item 1). While the jargon and technicality is tough to decipher for most users, it does have a particular effect: it serves to educate users who might not have the appropriate level of privacy protection knowledge and further place the onus on users to self-regulate privacy. The lack of knowledge, as well as the varying levels of trust, noticed in the user help forums does not result in Dropbox needing to update its services to better protect privacy but rather results in these marginal users being re-integrated into accordance with Dropbox’s privacy scripts and further responsibilized for personal privacy.

This process of re-integrating marginal users is crucial in understanding the de-scription of Dropbox. In going back and forth between the imagined users and the real users (Akrich 1992), it can be seen that while there is a clear standard user script communicated by Dropbox, actual users interact with this script in multiple ways. There is some level of stability in the competencies and behaviours of users of Dropbox, which is to be expected as the technology has moved passed its design stage and is incorporated into the everyday lives of millions of users. However, not all users adhere to these standard competencies, behaviours and user scripts. When users deviate from this standard, when they ‘slip between the cracks’ by not trusting Dropbox or having the knowledge to regulate their own privacy, the attempts to reintegrate these users involves an inherent tension between these users maintaining their marginality and the attempts of

the standard network to fully standardize use. Most users' interests have been translated such that they are aligned with those of Dropbox; however, the multiplicity and marginality of users must be further reduced in order to reduce the heterogeneity of the network, to demarcate user from non-user and to further stabilize and make durable Dropbox as a technological entity.

Breakdowns: The destruction of trust and the negotiation of privacy

Akrich (1992: 207) suggests that to fully understand the user scripts and de-scription of a given technological artefact, we should look for "disagreement, negotiation and the potential for breakdown." The latter is the most telling. In situations in which a technology breakdowns and ceases performing as expected, the taken-for-granted actions and competencies assumed by users or the technological artefact become questionable. When Dropbox breaks down, the unquestioned beliefs that users should trust the technology with security and handle all other privacy matters themselves begin to become observable. Dropbox's user scripts stop becoming accepted as necessary for use and begin to be contested. Users stop trusting the durability of Dropbox and start doubting whether Dropbox can and should do more to protect their private data. In other words, in situations of breakdown, privacy becomes negotiable.

Although the community help forums seem as they should present many examples of breakdowns – each new thread theoretically presents a problem that a user is having with the technology – these situations are not necessarily breakdowns in the sense that Akrich (1992) discusses. These minor problems do not involve the user scripts of a technology becoming negotiated and debated. As we have seen above, these simply represent the multiplicity of users, their values of trust and their knowledge of privacy

protection. They involve efforts by Dropbox and its associated actants (other users) to reintegrate these marginal users to further reduce heterogeneity and stabilize the user scripts. Nevertheless, some situations in which a severe breakdown occurs in which these user scripts become destabilized; they challenge the fundamental tenet of Dropbox's user scripts: trust in the object.

In particular, there are two breakdowns that are discussed in the forums: Dropbox being potentially implicated in the NSA PRISM surveillance program and some technical bugs suffered by Dropbox. When news of these breakdowns became known to users, several new threads were started to discuss these problems. For instance, in September 13th, three similar threads were started regarding PRISM: 'the NSA is planning to add Dropbox as a PRISM provider' (item 62), 'Dropbox please respond to PRISM allegations' (item 22), and 'NSA, PRISM, and Dropbox. Answered Questions and a WakeUp to Dropbox' (item 41). Several other threads involved users claiming they were leaving Dropbox after hearing the PRISM allegations; for example, one user simply titles the thread: 'I'm out (Post-Snowden) (item 31). Similarly, one of the longest threads in the forums, 'Drop box web interface was WIDE OPEN for some time yesterday' (item 15) involved a discussion of one of the technical bugs Dropbox suffered allowing any user to sign into any account using any password.

While reactions to these breakdowns varied greatly (as seen above, some users simply announced their departure from the service), they can generally be categorized under two themes: doubt and privacy protection. The former involves users expressing doubt and mistrust towards Dropbox and its ability to keep user data secure. This is perhaps best encapsulated by a user named Xyseven who, in response to Dropbox's

alleged future involvement in PRISM, simply asks “How secure is Dropbox” (item 62). Security, a competency that Dropbox takes responsibility and that is to be unquestioned and trusted by users, suddenly becomes questionable and contested. The result is mistrust in Dropbox and its security procedures; there is some doubt as to whether Dropbox is the durable object it is intended to be. For example, Xyseven in the same thread asks “if someone broke into or in any way gained access to your servers would it be possible for them to read the document or see the picture? If the answer is no, how can I trust you after what has been partially [revealed]?” Here, it can be seen how a central tenet of Dropbox – its security and impenetrability – is questioned and Dropbox’s response to these problems is already greeted with mistrust before such a response is given.

Similar responses are given to the technical bugs that Dropbox suffers. For example, Andrew M. states: “Allowing unlimited public access to everyone's private files is not a ‘brief glitch’, it's a ‘major and total security failure’” (item 15). Once again, Dropbox’s security which according to the expected user behaviours and user scripts is supposed to be taken for granted is challenged by a user. This technical bug is taken as a cue to question all aspects of Dropbox’s previously unquestionable security and technical expertise, which is best summarized by a quip from Alex N.: “If Dropbox can't do basic testing on their authentication screen after an update then what else is wrong with Dropbox” (item 15). Further mistrust and doubt towards Dropbox, its technological resources and expertise and most importantly, its communication and response to the technical bug are expressed by several users. For instance, Jonathan R. writes “This "glitch" and the handling of it sets an alarming precedent. To have the glitch is one thing,

but for us not to find out about it until we stumble across it on forum posts or third-party blog sites demonstrates an attitude towards customers that I didn't expect from Dropbox" (item 15), while Phillippe S. expresses some doubt towards how Dropbox handles situations that challenge its perceived durability: "I'm not sure the DB team would have even posted anything about the issue if some users didn't report it in the first place" (item 15).

It must be noted that while several users express these attitudes of doubt and mistrust, some users do not. Some users continue to conform to Dropbox's user scripts, arguing for a fervent self-regulation of privacy. Some users even take these news stories as proof of the need for self-regulation; for example, one of the stronger adherents to this point of view, a user named Richard P. claims "if you took some responsibility for your own security, this would be a non-issue" (item 62). Nevertheless, in the threads discussing Dropbox's breakdowns, this position is the minority. There is debate amongst users who hold this position versus the majority of users who express some doubt towards Dropbox. The second theme noticed in these threads, privacy protection, comes through particularly well in one such debate. In a thread discussing the PRISM allegations, Richard P. holds a debate with several other forum users who take the position that Dropbox should do more, should be more accountable in protecting users' privacy. Privacy is not taken as something that users are responsible to self-govern and take for granted inasmuch as it involves Dropbox. The manner that privacy is to be protected is not left up to the user, but becomes negotiated, debated and contested. In other words, a central tenet of Dropbox's user script becomes discarded and re-negotiated.

This debate and negotiation involves Richard P. holding to the self-governance position: “Stop expecting other people to protect *your* privacy, that's something *you* need to do” (item 22). Several users respond with alternate positions. For instance, Andrew M. asks: “How are we supposed to protect *our* privacy when the government is secretly (and un-[constitutionally]) monitoring almost every form of communication or even action we make” (item 22). Andrew M. later adds “you suggest that I encrypt every single phone call and text message I send too? If I don't do that am I voluntarily giving up my privacy?” (item 22) to which Richard P. provides the following response:

> If you are TRUSTING a third party, be it Dropbox, your ISP, your network provider, the USPS or ANYONE ELSE, then you are voluntarily giving up your privacy to the extent at which you can force them to NOT DO THINGS.
> What about this is so freaking hard? If you voluntarily and willingly hand over all your personal crap to a third party without taking even a modicum of responsibility for it yourself, then you have NO ONE BUT YOURSELF to blame when that third party is obliged to hand your information over to someone else. (item 22)

Here, it can be seen how Richard P. is a user who conforms to Dropbox’s ideal user, even in times of breakdown. He views Dropbox as an object, who is ‘obliged’ to perform certain actions. Users, on the other hand, are subjective, prone to error and to blame for the infringement of their own privacy. Thus, the onus of privacy protection remains on the user.

This debate continues with other users participating and challenging this idea that privacy protection is the responsibility of the user. For example, David R. adds:

> there are different levels of trust. Only the most paranoid would exclude all third party services. At some point you have to trust something… A blanket condemnation of all who expect a service to fulfill [its] contractual obligations is not only unhelpful, but it misdirects concerns away from where it can do actual good, i.e. what we do and do not allow in this country... We are responsible for our privacy, yes, but in that we are also responsible for what our representatives do in our name. The answer in a democracy is not pulling into one's own shell,

> trusting no one, it is to make changes to the laws and restrict what governing agencies are allowed to do. (item 22)

Several important ideas come through in this response. First, David R. does not necessarily express doubt or mistrust in Dropbox; in fact, he admits that there must be some level of trust in and delegation of action to technological entities in order to function. Nevertheless, he challenges the idea that users are solely responsible for privacy protection and that breakdowns simply test the success of users' self-governance. Rather, Dropbox should assume some responsibility, to be prescribed by law in the vision of David R., for the protection of personal privacy.

Conclusion: Opening the black box and negotiating privacy

Thus, what we see here is a negotiation of privacy and privacy protection. As seen in Chapter Four, according to Dropbox's user scripts, privacy protection is something that is the responsibility of the user. In times when Dropbox runs smoothly, this is not questioned. As this chapter has shown, for the most part, Dropbox users are stable. Some marginal users exist who have varying levels of trust and knowledge to protect their own private material; however, other users are quick to reintegrate these users into the standard fold. All this changes in moments of breakdowns. Users cease trusting Dropbox, and mostly reject the notion that privacy protection is something that they are responsible for by debating what it means for something to be privacy, what it means to trust another party with one's privacy, and what that party should be legally bound to do to protect this privacy.

In moments of smooth operations, privacy is almost absent – not in the sense that there is no privacy, but in the sense that it is not questioned, taken for granted and seemingly a non-issue. There exists a standard user script regarding privacy – what is

private and how it should be protected is not contested. However, when the trust in Dropbox is destroyed in moments of breakdown, this changes. These user scripts and delegation of particular actions rest on trust in the objectivity of a technological entity. When the apparent rigidity and durability of the technological entity is questioned and as a result, these user scripts fall apart. The efforts of Dropbox to responsibilize the user become undone and a debate as to how privacy is to be protected emerges. In other words, when trust disappears, privacy (or the lack of privacy) appears.

The black box once again provides a useful metaphor for this phenomenon. As I have discussed throughout this project, the black box's internal workings are not questioned; they are trusted. However, when the black box breaks down, its internal workings become noticeable (Akrich 1992). The black boxed technology has standard user scripts or conditions of use, and will produce consistent outputs. Dropbox can represent such a black box. When it is running smoothly, its internal security mechanisms are simply trusted. There is a standard, stable set of user scripts that outline that users are meant to protect privacy. Dropbox's output is simple: it will keep user data secure. There is a clear distinction between privacy protection as the responsibility of users, and security as something durable and the responsibility of the technological entity. However, in moments of breakdown, we can open this black box. When Dropbox's security and smooth operations are questioned, when the trust in this black box's internal workings is destroyed, this clear delegation of action becomes cloudy. The rights and responsibilities of various actors – users, Dropbox, governing agencies – become debated and contested.

6 Discussion

What are some repercussions of this analysis of Dropbox, users, cloud computing, and data privacy? On a superficial level, my findings may seem self-evident: a technology company tells its users what it expects of them and users for the most part agree, so long as the technology holds up. However, if we dig deeper, we can extract some important implications from this research. Following the work of other scholars who look at trust in information and communications technologies, I believe that trust is a more useful concept for studying the implications of new technologies than simply looking at privacy.

In Chapter Two, I found that there is a dearth of existing literature on cloud computing and data privacy that examines the role of user agency and that trust is one conceptual tool to avoid this problem. In Chapter Three, I outlined how – using principles from actor-network theory – one could study trust and reimagine the role of user agency in discussing cloud computing. In particular, I outlined the methodological principles of Akrich's (1992; Akrich and Latour 1992) user scripts and de-scription and the principle of co-production to look at how users and technologies are mutually working on each other. In applying these principles to my case study in Chapters Four and Five, I found that Dropbox prescribed trust and privacy protection on its users, while maintaining security as its domain. Users, for the most part, accepted this script; however, some varying levels of trust were observed in users. What was noteworthy about the analysis in Chapter Five, however, was how in instances of breakdown, these user scripts and trust fall to pieces. This has led me to the conclusion that only when trust

is shattered does privacy and the trade-off of personal privacy for use become contested and negotiable.

However, what makes this analysis different than other literature on trust – and what this project is ultimately about on a theoretical level – is the nexus of technology, objectivity and trust. A word about each and how they relate is necessary. My analysis and understanding of technology rests on many of the assumptions of actor-network theory, and particularly Bruno Latour's (1991) quip: "Technology is society made durable." I have extensively used the metaphor of the black box to exemplify this principle and stay faithful to the central tenets of ANT. The black box represents a network of associated humans and non-humans that has *stabilized such that its heterogeneity is reduced and it appears as a homogenous whole*. Its associations (i.e., its social relations) are hidden and become a durable technological entity. Users of this black boxed technology must not understand, follow or even be aware of the internal workings and associations but only need to understand how to use the black box as a whole; they only need to follow the user scripts and interact with the technology's user interface.

My example of cloud computing, and more specifically Dropbox, can highlight this principle. As discussed in the introduction, cloud computing is a great example of a heterogeneous assemblage. It is not a simple technological artefact but is rather an *idea* that encompasses a wide range of computing programs, hardware and human actors in order to be realized. Through my analysis of users of Dropbox, I have found that many of these users simply accept the user scripts of this program; they interact with Dropbox as a black boxed technology. They do not need to question or understand how Dropbox

or how cloud computing more generally functions, they just need to know how to interact with Dropbox's user interface. To them, Dropbox is a program to store and synchronize files to be accessed at a later date, not a heterogeneous network of associated human and non-human actants.

In studies of black boxed technologies, objectivity is always implicit but rarely explicitly discussed. Part of this is likely due to the self-evidence of the objectivity of black boxed technologies. Technological entities are objective in multiple senses of the word: one, they are objects; and two, they behave consistently. Users of a black boxed technology who behave in accordance with the user scripts should expect the technology to behave the same way every time. Its internal workings and associations are reduced such that users provide an input and expect consistent outputs from the black box. The objectivity of technologies is, in this sense, very self-explanatory. Nevertheless, using the metaphor of the black box highlights a key point about the nexus between objectivity and technology: objectivity is an effect of a network or association's durability and stabilization. It is precisely when a network becomes black boxed that it becomes seen as objective. It is when those contingent associations and subjective actors are reduced (in other words, when the social has been reduced) that a technology that behaves consistently and objectively appears.

When exploring technology and objectivity in this way, it is possible to conceptualize the understanding of trust I have put forth in this analysis. Trust simply becomes a necessary by-product of the stabilization and reduction of heterogeneous associations, and the perceived objectivity of a technological entity. Technologies, here understood as stabilized networks, objectivity and trust all necessitate one another. Black

boxed technologies are trusted to behave as expected, to behave objectively. If there is distrust in the technology, it is not perceived as completely objective; there is room for error. If the heterogeneity of a network is not completely reduced, there is more room for distrust as users must now trust each of the heterogeneous associations and not simply the homogenous black boxed technology. Thus, technology, objectivity and trust go hand in hand; they all appear simultaneously as a heterogeneous network is reduced, stabilized and made durable. My findings, in Chapter Four and particularly Chapter Five thus suggest that Dropbox as a case study of cloud computing is not a completely stabilized technology, though it is well on its way. It is stable enough that users for the most part trust the technology and behave in accordance with its user scripts. However, there is still a concerted effort on the part of Dropbox to communicate its objectivity and trustworthiness and to further reduce its heterogeneity and the marginality of some users.

Limitations & Implications of this Study

While this project is an attempt to think about technology and trust in this way and explore its implications for data privacy, it undoubtedly has its limitations. First and foremost, my analysis represents only one case study, somewhat arbitrarily chosen, and only one interpretation of the data. As discussed in Chapters Four and Five, I did not follow any strict methodology of data analysis but rather interpreted the data while trying to be consistent with guidelines provided by Wodak and Meyer (2009) on critical discourse analysis and with principles outlined by ANT scholars. There was no external confirmation of my coding procedure and no attempt to ensure the study could be replicated. As such, this project cannot offer any concrete, valid, reliable and generalizable findings; rather, I prefer to consider my conclusions as one interpretation

amongst many possible ways to understand cloud computing, technology, trust and data privacy.

That being said, the purpose and implications of this study does not lie in its ability to make generalizable conclusions but precisely in its function as a thought experiment. As with other studies of technology in the ANT tradition, my goals were to 'open the black box' – to highlight the contingent associations, to trace the work down to stabilize these heterogeneities and to challenge taken for granted assumptions embedded within the technology. Latour (2004; 2005) offers one way of expressing this goal: by moving from 'matters of fact' to 'matters of concern'. By this, Latour refers to how the analyst should not treat black boxed ideas and technologies as taken for granted, stable entities but rather highlight the heterogeneity and constructed nature of these entities. Doing so makes a key difference in thinking about, contesting and regulating science, technology and objects: the focus ceases to be placed on a static entity that is sure to change and is placed on the dynamic *process* of how such an entity is formed, how it aligns different points of view and the effects this has on a given public or population.

As such, the implications of my study do not stem from an attempt to make a generalizable conclusion about trust and privacy in the world of cloud computing. Rather, I want to highlight that trust is an effect; trust appears when a cloud computing technology such as Dropbox is able to become somewhat stabilized, delineates clear user scripts and reduces its heterogeneity. In other words, users can only trust Dropbox as a homogenous and objective technology that keeps their data secure. My analysis in Chapter Five has shown that when the black boxed technology breaks down and users cease to trust Dropbox, the contingent nature of privacy protection and data security

come to the forefront. Furthermore, by treating cloud computing as a heterogeneous association, I am by definition, displaying some mistrust in the technology. I am 'opening the black box' and not treating it as a stable, durable, homogenous and objective protector of personal data.

This is an important practical implication of this analysis of cloud computing; it introduces some doubt and mistrust, and therefore allows privacy to become contestable without needing to wait for a situation of breakdown. Despite this, I do not believe this means that because cloud computing is to be treated with a bit of mistrust, it cannot be used. Since privacy becomes taken for granted when a certain level of trust is afforded to cloud computing, I believe users are better equipped to understand and protect their privacy with a bit of mistrust towards the technology. By being aware of the heterogeneities and the associations involved in cloud computing, by opening the black box and treating it as a matter of concern, users can make more educated decisions on who or what they want to entrust to protect their personal data. They do not necessarily need to trust 'the cloud' as a homogenous whole but can trust and delegate action to certain actants within this network. In Chapters Two and Three, I argued for a conceptual framework for understanding cloud computing in a way that respects user agency; the ultimate practical implication of this theoretical goal is this increased choice opening the cloud computing black box grants to users. In other words, by opening the black box, users are not deferring all action to a homogenous, expert third party but remain, in part, experts of their own privacy who are able to act as autonomous agents to protect their data.

That being said, some level of trust in the technology is required in order to use cloud computing services. Thus, like Star (1991), my goals could be said to provide the conceptual and theoretical tools for users to retain their marginality in relation to a standardized technology as much as possible. Thus, while I argue that the practical implications of such an analysis lie in its ability to add a touch of mistrust in the minds of users, I believe the important policy implication is the ways in which trust can be established, maintained and nurtured. I began this thesis with a brief discussion of the Office of the Privacy Commissioner's (2011) consultations on cloud computing and the protection of privacy, which seems a useful place to end. At times in this report, the OPC takes the approach of looking for ways to adapt regulation to a new technology such as cloud computing. They are hardly alone in this approach; most policy questions surrounding cloud computing can, in one way or another, fit with this approach. However, in accordance with the goal of treating cloud computing as a 'matter of concern' and focusing on the dynamic process by which it changes, aligns different points of view and associates various actors, policy questions should be less oriented towards technical safeguards for protecting private data and more oriented towards *accountability* of those actors whom are to be trusted with privacy protection. However, these sorts of policy questions are outside of the scope of this project; while I have attempted to offer an alternative way to conceptualize the complex relationship between cloud computing, data privacy and trust, more research, such as that of Bansal and his colleagues (2010; 2008), on explaining the nature of this trust and how it can nurtured through accountability policy is needed.

References

"Canadian Charter of Rights and Freedoms."1982. *S 2, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK)*.

Albrechtslund, Anders. 2012. "Socializing the City: Location Sharing and Online Social Networking." Pp. 187-197 in *Internet and Surveillance: the challenges of Web 2.0 and social media*, edited by C. Fuchs, K. Boersma, A. Albrechtslund and M. Sandoval. New York: Routledge.

Allmer, Thomas. 2012. "Critical Internet Surveillance Studies and Economic Surveillance." Pp. 124-146 in *Internet and Surveillance: the challenges of Web 2.0 and social media*, edited by C. Fuchs, K. Boersma, A. Albrechtslund and M. Sandoval. New York: Routledge.

Akrich, Madeleine. 1992. "The De-Scription of Technical Objects." Pp. 205-224 in *Shaping technology/building society: studies in sociotechnical change*, edited by W.E. Bijker and J. Law. Cambridge: MIT Press.

Akrich, Madeleine and Bruno Latour. 1992. "A Summary of a Convenient Vocabulary for the Semiotics of Human and Nonhuman Assemblies." Pp. 259-264 in *Shaping technology/building society: studies in sociotechnical change*, edited by W.E. Bijker and J. Law. Cambridge: MIT Press.

Andrejevic, Mark. 2012. "Exploitation in the Data Mine." Pp. 71-88 in *Internet and Surveillance: the challenges of Web 2.0 and social media*, edited by C. Fuchs, K. Boersma, A. Albrechtslund and M. Sandoval. New York: Routledge.

Andrejevic, Mark. 2007. *iSpy: surveillance and power in the interactive era*. Lawrence, Kan: University Press of Kansas.

Anton, A. I., J. B. Earp and J. D. Young. 2010. "How internet users' privacy concerns have evolved since 2002." *IEEE Security & Privacy Magazine* 8(1):21-27.

Arditi, David. 2012. "Disciplining the Consumer: File-Sharers under the Watchful Eye of the Music Industry." Pp. 170-186 in *Internet and Surveillance: the challenges of Web 2.0 and social media*, edited by C. Fuchs, K. Boersma, A. Albrechtslund and M. Sandoval. New York: Routledge.

Bansal, Gaurav, Fatemeh Mariam Zahedi, and David Gefen. 2008. “The Moderating Influence of Privacy Concern on the Efficacy of Privacy Assurance Mechanisms for Building Trust: A Multiple-Context Investigation.” Presented at the Proceedings of 29th International Conference on Information Systems, December 14-17, Paris, France.

Bansal, Gaurav, Fatemeh Mariam Zahedi, and David Gefen. 2010. “The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online.” *Decision Support Systems* 49(2): 138-150.

Barry, Andrew. 2001. *Political Machines: governing a technological society.* New Brunswick, NJ: Athlone Press.

Barry, Andrew. 2002. "The anti-political economy." *Economy and Society* 31(2):268-284.

Benkler, Yochai. 2006. *The Wealth of Networks: how social production transforms markets and freedom.* New Haven: Yale University Press.

Bennett, Colin. 1991. "Computers, Personal Data, and Theories of Technology: Comparative Approaches to Privacy Protection in the 1990s." *Science, Technology & Human Values* 16(1):51-69.

Bianco, Jamie S. 2009. "Social Networking and Cloud Computing: Precarious Affordances for the "Prosumer"." *Women's Studies Quarterly* 37(1-2):303-312.

Bijker, Wiebe E. 2007. “Dikes and Dams, Thick with Politics.” *Isis* 98(1): 109-123.

Bijker, Wiebe E. and John Law. 1992. *Shaping technology/building society: studies in sociotechnical change*. Cambridge: MIT Press.

Boczkowski, Pablo and Leah A. Lievrouw. 2008. "Bridging STS and Communication Studies: Scholarship on Media and Information Technologies." Pp. 949-978 in *The Handbook Of Science And Technology Studies*, edited by E.J. Hackett, O. Amsterdamska, M.E. Lynch and J. Wajcman. Cambridge: MIT Press.

Bodle, Robert. 2011. "Privacy and Participation in the Cloud: Ethical Implications of Google's Privacy Practices and Public Communications." Pp. 155-174 in *The ethics of emerging media: information, social norms, and new media technology*, edited by B. Drushel and K.M. German. New York: Continuum.

Bok, Sissela. 1983. *Secrets: On the Ethics of Concealment and Revelation.* New York: Pantheon Books.

Carr, Nicholas G. 2008. *The Big Switch: rewiring the world, from Edison to Google.* New York: W. W. Norton & Company.

Callon, Michel. 1980. “Struggles and Negotiations to define what is Problematic and what is not: the Sociology of Translation.” Pp. 197-219 in *The Social Process of Scientific Investigation: Sociology of the Sciences Yearbook*, *Volume 4*, edited by K. D. Knorr, R. Krohn and R. D. Whitley. Dordrecht and Boston, MA: Reidel.

Callon, Michel. 1986. "Some elements of a sociology of translation: domestication of the scallops and the fishermen of St. Brieuc Bay." Pp. 196-233 in *Power, Action and Belief: A New Sociology of Knowledge*, edited by J. Law. London: Routledge & Kegan Paul.

Callon, Michel and John Law. 1982. "On Interests and their Transformations: Enrollment and Counter-Enrollment." *Social Studies of Science* 12:615-625.

Cavoukian, Ann. 2008. *Privacy in the Clouds: A white paper on privacy and digital identity, implications for the internet.* Toronto, Ont: Information and Privacy Commissioner/Ontario.

Center for Science and Innovation Studies. 2010. *Center for Science and Innovation Studies*. University of California, Davis. http://innovation.ucdavis.edu/. Retrieved February 13, 2014.

Chellappa, Ramnath K., and Raymond G. Sin. 2005. "Personalization Versus Privacy: An Empirical Examination of the Online Consumer's Dilemma." *Information Technology and Management* 6(2):181-202.

Christensen, Miyase and Andre Jansson. 2012. "Fields, Territories, and Bridges: Networked Communities and Mediated Surveillance in Transnational Social Space." Pp. 220-238 in *Internet and Surveillance: the challenges of Web 2.0 and social media*, edited by C. Fuchs, K. Boersma, A. Albrechtslund and M. Sandoval. New York: Routledge.

Clarke, Adele and Theresa Montini. 1993. "The Many Faces of RU486: Tales of Situated Knowledges and Technological Contestations." *Science, Technology & Human Values* 18(1):42-78.

Couillard, David A. 2008. "Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing." *Minnesota Law Review* 93:2205-2238.

Cronin, Mary J. 2000. "Privacy and Electric Commerce." Pp. 1-47 in *Public Policy and the Internet: privacy, taxes, and contract*, edited by N. Imparato. Stanford: Hoover Institution Press.

Das, Priya, H. W. Classen and Raj Davé. 2013. "Cyber-Security Threats and Privacy Controls for Cloud Computing, Emphasizing Software as a Service." *Computer & Internet Lawyer* 30(3):20-24.

DeCew, Judith W. 1997. *In Pursuit of Privacy: law, ethics, and the rise of technology.* Ithaca: Cornell University Press.

Dropbox. 2013, April 10. *Privacy Policy*. https://www.dropbox.com/privacy. Retrieved December 7, 2013.

Dropbox. 2012, August 27. *Another layer of security for your Dropbox account*. https://blog.dropbox.com/2012/08/another-layer-of-security-for-your-dropbox-account/. Retrieved December 7, 2013.

Dropbox. 2012, March 26. *Terms of Service*. https://www.dropbox.com/terms. Retrieved December 7, 2013.

Dropbox. 2011, July 1. *Changes to our policies (updated).* https://blog.dropbox.com/2011/07/changes-to-our-policies/. Retrieved December 7, 2013.

Dropbox. 2011, June 20. *Yesterday's Authentication Bug.* https://blog.dropbox.com/2011/06/yesterdays-authentication-bug/. Retrieved December 7, 2013.

Dropbox. 2011, April 21. *Privacy, Security & Your Dropbox (Updated)*. https://blog.dropbox.com/2011/04/privacy-security-your-dropbox/. Retrieved December 7, 2013.

Dropbox. N.d.a. *Acceptable Use*. https://www.dropbox.com/acceptable_use. Retrieved December 7, 2013.

Dropbox. N.d.b. *Security Overview*. https://www.dropbox.com/security. Retrieved December 7, 2013

Durkheim, Emile. 1933 [1893]. *The division of labor in society*. New York: Free Press.

European Union. 2000. "Charter of Fundamental Rights of the European Union." *Official Journal of the European Communities, 18 December 2000 (OJ C 364/01)*.

Fernback, Jan and Zizi Papacharissi. 2007. "Online privacy as legal safeguard: the relationship among consumer, online portal, and privacy policies." *New Media & Society* 9(5):715-734.

Flaherty, David. 1986. "Governmental Surveillance and Bureaucratic Accountability: Data Protection Agencies in Western Societies." *Science, Technology, & Human Values* 11(1):7-18.

Fried, Charles. 1990. "Privacy." Pp. 51-67 in *Computers, Ethics & Society*, edited by M.D. Ermann, M.B. Williams and C. Gutierrez. New York: Oxford University Press.

Fuchs, Christian. 2012. "Critique of the Political Economy of Web 2.0 Surveillance." Pp. 31-70 in *Internet and Surveillance: the challenges of Web 2.0 and social media*, edited by C. Fuchs, K. Boersma, A. Albrechtslund and M. Sandoval. New York: Routledge.

Fuchs, Christian, Kees Boersma, Anders Albrechtslund and Marisol Sandoval, eds. 2012. *Internet and Surveillance: the challenges of Web 2.0 and social media*. New York: Routledge.

Gellman, Barton and Laura Poitras. 2012. "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program." *The Washington Post,* June 6th, 2012.

Giddens, Anthony. 1990. *The consequences of modernity.* Stanford: Stanford University Press.

Grodzinksy, Frances and H. T. Tavani. 2011. "Privacy in "the Cloud": Applying Nissenbaum's Theory of Contextual Integrity." *ACM SIGCAS Computers and Society* 41(1):38-47.

Haraway, Donna J. 1991. *Simians, cyborgs and women : the reinvention of nature*. London: Free Association Books.

Harbison, Niall. 2011. "The Dropbox PR Fiasco - From Zero to Hero in 24 Hours." Simply Zesty, Retrieved June 2, 2013. (http://www.simplyzesty.com/Blog/Article/June-2011/The-Dropbox-PR-Fiasco-From-Hero-To-Zero-In-24-Hours).

Helms, Shawn C. 2001. "Translating Privacy Values with Technology." *Boston University Journal of Science and Technology Law* 7: 288:326.

Hibbert, Richard A. 2009. "Ethnomethodology and Social Theory." Pp. 159-178 in *The new Blackwell companion to social theory*, edited by B.S. Turner. West Sussex, UK: Wiley-Blackwell.

Jaegar, Paul T., Jimmy Lin, Justin M. Grimes and Shannon N. Simmons. 2009. "Where is the cloud? Geography, economics, environment and jurisdiction in cloud computing." *First Monday* 14(5).

Jaeger, Jaclyn. 2013. "Big Data Privacy Standards Moving Forward." *Compliance Week* 10(109):40-41.

Jasanoff, Sheila. 2004. "The idiom of co-production." Pp. 1-12 in *States of Knowledge: the co-production of science and social order*, edited by S. Jasanoff. New York: Routledge.

Jones, William P. 2012. *The future of personal information management*. San Rafael, CA: Morgan & Claypool.

Kimrey, Blaine and Bryan Clark. 2012. "Cyberprivacy and Digital Privacy Risks." *Communications Lawyer* 29(2):10-16.

Kline, Ronald and Trevor Pinch. 1996. “Taking the Black Box off its Wheels: The Social Construction of the Automobile in Rural America.” *Technology and Culture* 37:776-795.

Latour, Bruno. 1987. *Science in Action : how to follow scientists and engineers through society*. Philadelphia: Open University Press.

Latour, Bruno. 1988. *The Pasteurization of France.* Cambridge, MA: Harvard University Press.

Latour, Bruno. 1991. "Technology is society made durable." Pp. 103-131 in *A Sociology of Monsters: essays on power, technology, and domination*, edited by J. Law. London: Routledge.

Latour, Bruno. 1992. "Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts." Pp. 225-258 in *Shaping technology/building society: studies in sociotechnical change*, edited by W.E. Bijker and J. Law. Cambridge: MIT Press.

Latour, Bruno. 2004. "From Realpolitik to Dingpolitik – An Introduction to Making Things Public. " In *Making Things Public: Atmospheres of Democracy*, edited by B. Latour and P. Weibel. Cambridge: MIT Press.

Latour, Bruno. 2005. *Reassembling the Social: An introduction to actor-network-theory.* Oxford: Oxford University Press.

Latour, Bruno and Steve Woolgar. 1979. *Laboratory Life: the Social Construction of Scientific Facts.* Beverly Hills and London: Sage.

Law, John. 1987. "Technology and heterogeneous engineering: the case of Portuguese expansion." Pp. 111-134 in *The social construction of technological systems: new directions in the sociology and history of technology*, edited by W.E. Bijker, T.P. Hughes and T.J. Pinch. Cambridge: MIT Press.

Law, John, ed. 1991. *A Sociology of Monsters: essays on power, technology, and domination*. London: Routledge.

Law, John. 2009. "Actor-Network Theory and Material Semiotics." Pp. 141-158 in *The new Blackwell companion to social theory*, edited by B.S. Turner. West Sussex, UK: Wiley-Blackwell.

Law, John and John Hassard. 1999. *Actor-Network Theory and After*. Oxford and Keele: Blackwell and the Sociological Review.

Levine, Donald. 1971. "Introduction." Pp. ix-lxv in *On individuality and social forms; selected writings*, edited by D. Levine. Chicago: University of Chicago Press.

Luhmann, Niklas. 1979 [1973, 1975]. *Trust and Power.* Chichester: Wiley.

Marx, Gary T. 2005. "Soft Surveillance: Mandatory Voluntarism and the Collection of Personal Data." *Dissent* 52(4):36-43.

Mather, Tim, Subra Kumaraswamy and Shahed Latif. 2009. *Cloud security and privacy*. Cambridge: O'Reilly.

Metzger, Miriam J. 2004. "Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce." *Journal of Computer-Mediated Communication* 9(4): DOI: 10.1111/j.1083-6101.2004.tb00292.x.

Monahan, Torin. 2006. *Surveillance and Security: technological politics and power in everyday life*. New York: Routledge.

Moser, Ingunn. 2000. "Against normalisation: subverting norms of ability and disability." *Science as Culture* 9(2):201-240.

Moser, Ingunn and John Law. 2001. *"Making voices": New Media Technologies, Disabilities, and Articulation*. Lancaster University: Centre for Science Studies and the Department of Sociology.

National Institute of Standards and Technology. 2011. *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*. U.S. Department of Commerce.

Office of the Privacy Commissioner of Canada. 2011. *Report on the 2010 Office of the Privacy Commissioner of Canada's consultations on online tracking, profiling and targeting, and cloud computing*. Ottawa: Government of Canada. Retrieved March 11, 2013.

Oudshoorn, Nelly and Trevor Pinch, eds. 2003. *How Users Matter: the co-construction of users and technologies*. Cambridge: MIT Press.

Parliament of Canada. *Personal Information Protection and Electronic Documents Act*. S.C. 2000, c. 5. 36th Parliament, 2000.

Radin, Margaret J. 2000. "Retooling Contract for the Digital Era." Pp. 115-149 in *Public Policy and the Internet: privacy, taxes, and contract*, edited by N. Imparato. Stanford: Hoover Institution Press.

Rose, Nikolas S. 1999. *Powers of Freedom: reframing political thought*. Cambridge: Cambridge University Press.

Ryan, Patrick and Sarah Falvey. 2012. "Trust in the clouds." *Computer Law & Security Review* 28(5):513-521.

Samuelson, Pamela. 2000. "Privacy As Intellectual Property?" *Stanford Law Review* 52(5):1125-1173.

Samson, Ted. 2012. "Dropbox fiasco serves as reminder of cloud-storage insecurity." InfoWorld, Retrieved June 2, 2013 (http://www.infoworld.com/t/cloud-security/dropbox-fiasco-serves-reminder-of-cloud-storage-insecurity-199197).

Sandoval, Marisol. 2012. "A Critical Empirical Case Study of Consumer Surveillance on Web 2.0." Pp. 147-169 in *Internet and Surveillance: the challenges of Web 2.0 and social media*, edited by C. Fuchs, K. Boersma, A. Albrechtslund and M. Sandoval. New York: Routledge.

Seidman, Steven. 1994. *The postmodern turn : new perspectives on social theory*. Cambridge ; New York: Cambridge University Press.

Sennett, Richard. 1998. *The Corrosion of Character: the personal consequences of work in the new capitalism*. New York: Norton.

Simmel, Georg. 1918. *Lebensanschauung*. Munich and Leipzig: Duncker & Humblot.

Smith, H. Jeff, Tamara Dinev, and Heng Xu. 2011. "Information Privacy Research: An Interdisciplinary Review." *MIS Quarterly* 35(4): 989-1015.

Star, Susan L. 1991. "Power, technology and the phenomenology of conventions: on being allergic to onions." Pp. 26-56 in *A Sociology of Monsters: essays on power, technology, and domination*, edited by J. Law. London: Routledge.

Sztompka, Piotr. 1999. *Trust: A Sociological Theory*. Cambridge: Cambridge University Press.

Taddicken, Monika. 2012. "Privacy, Surveillance, and Self-Disclosure in the Social Web." Pp. 255-272 in *Internet and Surveillance: the challenges of Web 2.0 and social media*, edited by C. Fuchs, K. Boersma, A. Albrechtslund and M. Sandoval. New York: Routledge.

Tavani, H. T. 2008. "Informational privacy: concepts, theories and controversies." Pp. 131-169 in *The Handbook of Information and Computer Ethics*, edited by K.E. Himma and H.T. Tavani. Hoboken, NJ: John Wiley and Sons.

Thomson, Judith J. 1975. "The Right to Privacy." *Philosophy & Public Affairs* 4(4):295-314.

Tierney, Thomas F. 1993. *The Value of Convenience: a genealogy of technical culture*. Albany: State University of New York Press.

Trottier, Daniel and David Lyon. 2012. "Key Features of Social Media Surveillance." Pp. 89-105 in *Internet and Surveillance: the challenges of Web 2.0 and social media*, edited by C. Fuchs, K. Boersma, A. Albrechtslund and M. Sandoval. New York: Routledge.

van Oost, E. 2003. "Materialized Gender: How Shavers Configure the User's Feminity and Masculinity." Pp. 193-208 in *How Users Matter: the co-construction of users and technologies*, edited by N. Oudshoorn and T. Pinch. Cambridge: MIT Press.

Walters, William. 2012. *Governmentality: critical encounters*. New York: Routledge.

Winner, Langdon. 1993. "Upon Opening the Black Box and Finding it Empty: Social Constructivism and the Philosophy of Technology." *Science Technology & Human Values* 8(3):362-378.

Wodak, Ruth and Michael Meyer. 2009. "Critical discourse analysis: history, agenda, theory and methodology." Pp. 1-33 in *Methods of critical discourse analysis*, edited by R. Wodak and M. Meyer. London: Sage.

Woolgar, Steve. 1991. "Configuring the user: the case of usability trials." Pp. 57-102 in *A Sociology of Monsters: essays on power, technology, and domination*, edited by J. Law. London: Routledge.

Zwick, Detlev, Samuel Bonsu and Aron Darmody. 2008. "Putting consumers to work: 'co-creation' and new marketing governmentality." *Journal of Consumer Culture* 8(2):163-196.

Appendix A: Dropbox Community Forum Threads

**All data retrieved on December 7, 2013.*

Item #	Title	URL
Item 1	"Recently Changed Files" - Make Optional or It's a Privacy Issue	https://forums.dropbox.com/topic.php?id=33469
Item 2	Ability to "password protect" Dropbox on a PC	https://forums.dropbox.com/topic.php?id=107528
Item 3	Add: Password protected settings	https://forums.dropbox.com/topic.php?id=99638
Item 4	Buying dropbox account from ebay: privacy question	https://forums.dropbox.com/topic.php?id=66214
Item 5	Can Dropbox Access My Stored Data??	https://forums.dropbox.com/topic.php?id=55207
Item 6	Can Dropbox really do what they want with our stuff?	https://forums.dropbox.com/topic.php?id=57599
Item 7	Can I password-protect the DB that is on my computer?	https://forums.dropbox.com/topic.php?id=91567
Item 8	CISPA and Dropbox	https://forums.dropbox.com/topic.php?id=59643
Item 9	Client-Side Encryption	https://forums.dropbox.com/topic.php?id=48652
Item 10	Corporate use / security concerns	https://forums.dropbox.com/topic.php?id=18880
Item 11	Deduplication - reports on privacy issues	https://forums.dropbox.com/topic.php?id=36365
Item 12	Delete the url dropbox.com from Desktop version at the panel or stop it to login	https://forums.dropbox.com/topic.php?id=103743
Item 13	Disappointed.	https://forums.dropbox.com/topic.php?id=51163
Item 14	Don't even know what to call it.	https://forums.dropbox.com/topic.php?id=57546
Item 15	Drop box web interface was WIDE OPEN for some time yesterday.	https://forums.dropbox.com/topic.php?id=40113
Item 16	Dropbox blocked by Internet Watch Foundation	https://forums.dropbox.com/topic.php?id=91216
Item 17	Dropbox can decrypt your (our) files!	https://forums.dropbox.com/topic.php?id=36814
Item 18	Dropbox changes policies / clarification / TOS UPDATED	https://forums.dropbox.com/topic.php?id=40765
Item 19	Dropbox Management Implicitly Violates Terms of Service	https://forums.dropbox.com/topic.php?id=58413

Item 20	Dropbox Privacy Concerns	https://forums.dropbox.com/topic.php?id=36835
Item 21	Dropbox searching through your files	https://forums.dropbox.com/topic.php?id=37902
Item 22	Dropbox, please respond to PRISM allegations.	https://forums.dropbox.com/topic.php?id=10154
Item 23	Email to Dropbox SOLVED!	https://forums.dropbox.com/topic.php?id=64265
Item 24	encrypted data and prism	https://forums.dropbox.com/topic.php?id=104501
Item 25	help me understand this security please...	https://forums.dropbox.com/topic.php?id=39262
Item 26	Help! IT is banning use of dropbox...	https://forums.dropbox.com/topic.php?id=64671
Item 27	how private is dropbox	https://forums.dropbox.com/topic.php?id=48694
Item 28	How secure are "shared" folders?	https://forums.dropbox.com/topic.php?id=52689
Item 29	I forgot to log out of my account on a friend's computer ...	https://forums.dropbox.com/topic.php?id=104589
Item 30	I have a few things to say	https://forums.dropbox.com/topic.php?id=38226
Item 31	I'm out (post-Snowden)	https://forums.dropbox.com/topic.php?id=104223
Item 32	Increase web privacy with random user id/key	https://forums.dropbox.com/topic.php?id=38214
Item 33	Information Governance and Dropbox	https://forums.dropbox.com/topic.php?id=100961
Item 34	Is Dropbox safe?	https://forums.dropbox.com/topic.php?id=44755
Item 35	Is Link in charge of Security and Privacy?	https://forums.dropbox.com/topic.php?id=64554
Item 36	Issue with Deleting Anything	https://forums.dropbox.com/topic.php?id=106575
Item 37	Letting others download my photos & vids	https://forums.dropbox.com/topic.php?id=107269
Item 38	MASSIVE SECURITY BREACH!	https://forums.dropbox.com/topic.php?id=107120
Item 39	New Links vs. Public Links and privacy concerns	https://forums.dropbox.com/topic.php?id=59018
Item 40	New Terms of Service	https://forums.dropbox.com/topic.php?id=40790
Item 41	NSA, PRISM and Dropbox. Answered Questions and a WakeUp to Dropbox!	https://forums.dropbox.com/topic.php?id=101833
Item 42	PC Security	https://forums.dropbox.com/topic.php?id=64609

Item 43	Possible security breach - account hacked	https://forums.dropbox.com/topic.php?id=98067
Item 44	Privacy	https://forums.dropbox.com/topic.php?id=36684
Item 45	Privacy	https://forums.dropbox.com/topic.php?id=50517
Item 46	Privacy	https://forums.dropbox.com/topic.php?id=51283
Item 47	Privacy Settings	https://forums.dropbox.com/topic.php?id=38795
Item 48	Privacy on My Work Computer?	https://forums.dropbox.com/topic.php?id=34659
Item 49	Privacy Problem	https://forums.dropbox.com/topic.php?id=63196
Item 50	Privacy question from new user	https://forums.dropbox.com/topic.php?id=103853
Item 51	Quick question about privacy	https://forums.dropbox.com/topic.php?id=38478
Item 52	Search within files	https://forums.dropbox.com/topic.php?id=107174
Item 53	Security	https://forums.dropbox.com/topic.php?id=43744
Item 54	Security Concern: Dropbox Doesn't Always Use Proxy Settings in OSX	https://forums.dropbox.com/topic.php?id=49717
Item 55	Security Issues?	https://forums.dropbox.com/topic.php?id=40653
Item 56	Security on Dropbox.	https://forums.dropbox.com/topic.php?id=39272
Item 57	Sending invite and the email displaying my full name - PRIVACY!!	https://forums.dropbox.com/topic.php?id=29806
Item 58	Signed up for Dropbox using the wrong email account	https://forums.dropbox.com/topic.php?id=103937
Item 59	Spyware in Dropbox? If not then please explain this...	https://forums.dropbox.com/topic.php?id=33667
Item 60	Takedown request?	https://forums.dropbox.com/topic.php?id=81796
Item 61	Terms and Conditions	https://forums.dropbox.com/topic.php?id=40780
Item 62	The NSA is planning to add Dropbox as a PRISM provider. I want to know how you crypt my files?! nr.2	https://forums.dropbox.com/topic.php?id=101771
Item 63	Times are changing	https://forums.dropbox.com/topic.php?id=102054
Item 64	Using Dropbox with photobooth software?	https://forums.dropbox.com/topic.php?id=107293

Item 65	want to privacy protect folder that I can access from PC or Mac	https://forums.dropbox.com/topic.php?id=44353
Item 66	What does it take to get a response from Dropbox regarding a security breach??!!	https://forums.dropbox.com/topic.php?id=95891
Item 67	What Dropbox should do to achieve a security/convenience WIN/WIN	https://forums.dropbox.com/topic.php?id=40145
Item 68	Where are dropbox servers located and what is your stance on FISA and our security	https://forums.dropbox.com/topic.php?id=96137
Item 69	Why is Dropbox tracking my location?	https://forums.dropbox.com/topic.php?id=97270