Table of Contents

Introduction

The occasion for this book is the growing conflict between the call for a "data-driven" society on the one side and the demand for ensuring individual freedom, autonomy, and dignity by means of protecting privacy on the other. Gathering and exploiting data of all kinds in ever greater quantities promises to create value and efficiency in business, education, healthcare, social services, energy, transportation, and almost all other areas of society. But at the same time, fears of loss of privacy lead to ever more prohibitive regulations. The European Union offers a concrete example of this conflict. In the name of a single digital market, the European Commission proclaims that "the internet and digital technologies are transforming our world. But existing barriers online mean citizens miss out on goods and services, internet companies and start-ups have their horizons limited, and businesses and governments cannot fully benefit from digital tools."[1] Among the "existing barriers" are not only inadequate infrastructure and the many different legal frameworks in Europe but also the strong data-protection laws. While extolling the benefits of good infrastructure and free flows of information, the EU has at the same time ratified a new General Data Protection Regulation (GDPR). The GDPR takes a strong stand on privacy as a fundamental human right and prohibits, at least in principle and intention, any use of personal data that is not based on the informed consent of the "data subject" or is not anonymized. From the perspective of big data analytics, which does not allow for complete knowledge of uses of data in advance, and therefore prevents any consent of data use based on this kind of knowledge, the vision of a data-driven society becomes unrealizable. One cannot base the development of new knowledge and products and services on data, while at the same time prohibiting the gathering and use of data. This becomes especially embarrassing when it is a matter of developing *personalized* products and services in all areas while at the same time demanding that data be anonymized and strictly separated from any personal references. It would

1 | https://ec.europa.eu/commission/priorities/digital-single-market_en. Of course, this conflict is not merely European. The situation in the USA is not essentially different.

seem that we are entering the 21st Century with society divided into those who believe that as much information as possible should be integrated into decision-making in all areas and at all levels and those who believe that human freedom, autonomy, and even dignity depend on secrecy and the withholding of as much information as possible. This book is an attempt to analyze the causes of this deep conflict in Western societies. Furthermore, it attempts to offer a perspective on how we might move forward into a world which is at once based on data and on a self-understanding of the human individual as an informational self whose freedom and dignity do not depend on privacy.

The vision for the future we propose is entitled "Network Publicy Governance." At first glance, it is not apparent what this title has to do with privacy, individual liberty, and issues of social injustice. After all, where does the individual appear in this title? What about freedom and human dignity? Even if the subtitle, "On Privacy and the Informational Self" promises to address these issues, the major focus seems to be on networks, governance, and something called "publicy." What does network publicy governance, which suspiciously sounds like a merely technical or administrative problem, have to do with protecting privacy, freedom, and the dignity of individuals? These questions are legitimate, and at least one reason why we have chosen this somewhat unusual title is to provoke questions such as these. But this is not the only reason. The idea of network publicy governance is intended to be more than mere provocation. It is intended to reframe contemporary privacy discourse beyond the constraints of traditional dichotomies such as private vs. public, individual vs. society, and human vs. technology; that is, outside of and beyond the conceptual constraints of Western modernity.

Indeed, although the book is apparently about privacy and the human subject, the reader will look in vain for a discussion of these topics along the well-known lines of modern ontological, epistemological, and moral individualism. Focusing on network publicy governance intends to move away from the autonomous rational subject of Western Enlightenment as well as the free and unique individual of the Judeo-Christian-existentialist tradition. Both Cartesian mind/body dualism and Judeo-Christian internal immediacy clearly distinguish an inner realm of meaning that is essentially private from external reality. It is these forms of subjectivity that are implicitly or explicitly the central figures and starting point of most contemporary privacy discourse. For something essentially human to become something private, subjectivity or mind must first be separated from the rest of the world, from other people and things. There must be an inside and an outside. Mind must be ascribed to the inside. There must be a unique realm of meaning inside each one of us that is distinguished from everything that is outside or beyond this boundary. Only then does privacy become possible and only then can privacy be understood as a fundamental right to be protected by law. We will argue against the deeply

ingrained and enormously influential conviction of the bounded self. We will claim that what humans have become in the digital age could be called an "informational self." The informational self consists of information and, as we will see, information exists in networks that are not clearly bounded. Whereas it could be expected that one tackle the many problems facing individuals in the information age by emphasizing personal privacy management, we want to go exactly in the opposite direction by focusing on networks instead of individuals, publicy instead of privacy, and governance instead of government. In the digital age, personal privacy management becomes network publicy governance.

We will not rehearse the usual narrative of freedom, autonomy, and dignity in terms of inequalities and power struggles between weak individuals on the one side and overpowering corporations and governments on the other. Instead, we will attempt to reformulate these issues in terms of networks. Why networks? Castells (1996) has convincingly shown that we are entering into a global network society based on digital information technologies. The affordances of these technologies are so influential and pervasive, that networks are becoming the dominant form of social order. In the global network society, neither individuals, nor organizations, nor institutions, nor governments are basic units of social order. More radical even than Castells is the appraisal of contemporary society proposed by actor-network theory, or ANT as it is known.[2] ANT claims that society is a "collective" of many different actor-networks. In the radical formulation that ANT proposes, the network is the actor, and the social actor is always a network. Following ANT, we will claim that the primary unit of social order and the dominant form in which cooperative action takes place today, and in the future, are networks. This is the reason why privacy, as well as the self-understanding of the human as autonomous, free and/or rational subjectivity which is the basis of privacy discourse, need to be reformulated in terms of networks.

From the network perspective, social theory in general and privacy discourse, in particular, can no longer proceed from the assumption that we are dealing with clearly bounded unities, whether individual, organizational, or governmental. When actors become networks, that is, when actors are constituted in networks and exist as networks, then they enter into a condition that can be considered to be the "default" condition of humans in society. This condition, following Stowe Boyd, can be termed "publicy." Publicy is not publicity. It is not the state of being known, but the condition of being an *informational self*. In contrast to the essentially private individual of Western modernity, the informational self is not an isolated individual that somehow secondarily enters into social contracts, but a hybrid and heterogeneous ensemble of associations that are always already social. The informational self is constitutively linked

2 | See above all the work of Bruno Latour.

up to others, both human and nonhuman. Indeed, the self is inherently an ensemble of associations. That the self is made up of heterogeneous elements is in itself nothing new. Whether it be body and soul, reason and passion, good and evil, freedom and determinism, the Western self – both individual and collective – has always understood itself within the tension of opposing forces and qualities. Typical strategies of creating unity have been to subsume the particular under the universal as in Descartes *ego cogito*, or submit the whole contradictory lot to the fiat of absolute freedom as in existentialism, or even to confine mind to the material brain. The goal in all these cases is to construct a bounded unity. In distinction to this traditional notion of subjectivity, the informational self we are proposing is not a constructed unity, that is a system of parts integrated somehow into a whole, but a network of associations. It is one thing to impose unity upon diversity, and it is another thing to take account of as many diverse voices as possible through ongoing negotiations that never define clear boundaries. The informational self is based on the fact that the links that construct networks can be understood as the product of such negotiations which we call *information*. The network actor is an informational self because actor-networks are constituted by information. Information, we will argue, is neither rational nor irrational, neither public nor private. We will argue that the digital transformation has created a situation in which the informational self, whose default condition is publicy and not privacy, has increasingly come to the fore and is both theoretically and practically replacing the unitary and bounded individual of Western modernity.

The information age and the global network society have changed the playing field and the rules of engagement for conceptualizing subjectivity and protecting liberty, autonomy, dignity, and justice. In this situation, our long-cherished assumptions about self and society have become inadequate. The standard narrative of contemporary privacy rights, privacy legislation, privacy theory, and privacy strategies tells of an individual subject who is locked into a constant and futile struggle to maintain a balance of power against overwhelming social actors, usually personified in the form of large corporations and governments. In the information age, it seems that the only weapons at its disposal are withholding, disguising, and blocking flows of information. The futility, impracticability, and theoretical inconsistency of this struggle are indications that new thinking is needed. This book suggests a way out of the present standoff between information networks and private individuals by reframing not only the notion of network but also the self-understanding of the human and therefore the way in which privacy is understood. We attempt to place discussions of subjectivity, identity, and personhood on a different terrain, namely, on the terrain of networks. Instead of the autonomous, rational subject of the Western Enlightenment, or the absolute freedom of existentialism, we propose the informational self, and instead of privacy, we

offer publicy. We claim that by shifting the grounds of debate, we will be able to escape the fruitless opposition of private and public or individual and society that characterizes much present-day theory as well as practice.

To speak of the "informational self" is to locate information at the center of the human. This raises questions not only about the nature of human existence but also about the nature of information. What is information? Can information constitute the human? Whereas privacy was once a matter of protecting property and the sanctity of the home, today it is more and more conceived of in terms of information. Privacy has become an informational issue, a matter of "informational self-determination."[3] Privacy is the right to decide what information about oneself one wishes to communicate and what not. Not only that but in some more radical formulations, privacy is defined in terms of certain kinds of information or informational contents. It is supposed that some information about a person should never be communicated. This leads to the assumption that privacy rights are inalienable and fundamental rights that under no circumstances can be traded off for other rights or gains. In this view, which is typical of the European tradition, privacy has to do with information that is so intimate and personal that it demands to be protected regardless of any supposed advantages to giving it away. This "fundamentalist" view raises the question of the extent to which human beings are constituted by information, that is, as Floridi (2014) says, whether human beings are "inforgs." Inforgs are informational organisms which inhabit a world that is made up of information, the "infosphere." How is information to be understood such that human individuals and the entire world can be conceived of as in some way informational? If information is a fundamental ontological characteristic of the world, and if humans are indeed inforgs, what does this mean for privacy? Questions such as these do not usually stand at the beginning of legal or philosophical discussions of privacy. Nevertheless, privacy discourse today revolves around information, especially what is termed "personal information." This indicates that the fundamental question of the nature of information

3 | The term "informational self-determination" comes from German "*informationelle Selbstbestimmung*," which was used by the German Federal Constitutional Court (1983) in ruling that "[...] in the context of modern data processing, the protection of the individual against unlimited collection, storage, use and disclosure of his/her personal data is encompassed by the general personal rights of the German constitution. This basic right warrants in this respect the capacity of the individual to determine in principle the disclosure and use of his/her personal data. Limitations to this informational self-determination are allowed only in case of overriding public interest." In the USA, Westin's (1967: 2) famous definition of privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" comes closest to this idea.

should no longer be simply taken for granted when it comes to adequately conceptualizing privacy or human freedom, autonomy, and dignity. Not only privacy theory, but also an adequate self-understanding of the human should be based upon a coherent and appropriate theory of information. Only then can an understanding of privacy be developed that can move beyond the seemingly irresolvable conflicts that surround not only the theory, but also the way in which freedom, justice, and flows of information in the digital age are realized.

Part 1 of this book, therefore, begins with an attempt to define information. We will argue that information is not a semantic content. Information is not necessarily or essentially "about" anything or anyone. Instead, we propose a definition of information based upon actor-network theory in which information can be defined as that which links together actors into a network while at the same time constructing the roles and identities of these actors.[4] We propose interpreting Latour's principle of "irreduction" and what he describes as "technical mediation" in terms of a theory of information. Irreduction says that "nothing is, by itself, either reducible or irreducible to anything else" (Latour 1993: 158). Technical mediation describes what this cryptic statement means. Using the simple example of a stone ax, we will argue that technical mediation, that is, the mutual affordances of translation and enrollment that both human and nonhuman actors bring with them when humans use tools, or do anything for that matter, can be understood as the process of constructing information.

Translation and enrollment is the process of establishing links between humans and nonhumans in actor-networks in such a way that no actor is either reduced to another or completely independent. We will interpret technical mediation, or the making of associations, as an information process. If we recall Bateson's well-known definition of information as a difference that makes a difference, then from an ANT perspective, information is a difference *making* a difference. The emphasis is on the making, that is, the *process* of information construction. This process is the ongoing and ever-volatile dynamic of linking things together in such a way that something new comes into being. Information arises from the mutual and symmetrical construction of associations, interfaces, differences, and relations in the world. Indeed, it is information that makes the *world*, that is, the human world of meaning in which we live. This means that information is not a thing of some kind that could "belong" to any individual social actor. Information is much more like, but not the same as, a common good or a common-pool resource that neither belongs to individuals alone nor everyone equally. Information constitutes the network in which actors become who they are. With regard to privacy theory, this means

4 | In a previous work, "Organizing Networks" (Belliger/Krieger 2016) we argued that this is a "narrative" process. The focus here is not on narrative, but on what narratives are made of and which narrative we want to tell.

that even if it can be said that in some way information constitutes social actors, they do not "own" this information, nor are they *exclusively* constituted by it. Contrary to what traditional privacy theory assumes, individuals do not have sovereignty over information. They cannot unilaterally and without regard to all participants in a network create information, distribute it, withhold it, destroy it, or use it in any way they wish. This view of information has consequences for how privacy, as well as the exploitation of information in a digital world, can adequately be understood.

Part 2 of this book takes a deeper look at the reasons offered for privacy and the claims that are made for linking privacy to freedom, autonomy, and human dignity. There is no doubt that privacy matters in society, and perhaps more than ever in the digital age, but there is little consensus about why and how. We propose taking a fresh and unorthodox look at the meaning and value of privacy. We will naively ask the question: Who or what is privacy supposed to protect and why? To be sure, privacy is not a merely academic matter. Everyone is "personally" concerned. But are these concerns reasonable? Are they grounded in real threats or harms that could and do arise from flows of information? Does the free flow of information in itself violate property rights, endanger security, or even amount to a violation of fundamental human rights? Do freedom, autonomy, self-determination, and human dignity rest upon privacy? And if so, what kind of privacy? Do calls for a "data-driven" society, the advent of big-data, the lure of personalized products and services, and the seemingly inevitable advance of algorithmic automation in all areas of life necessarily threaten human integrity, freedom, and fundamental rights?

We will take a close look at the claims made both for an instrumental value for privacy as well as for privacy as a fundamental right in itself. The instrumental view, which is typical of American law and privacy theory, understands privacy as a value for ensuring other rights, such as property rights or the right to security. Privacy in this view is not a fundamental right in itself, but an instrument for protecting more basic rights. The European view, on the contrary, is anchored in the Universal Declaration of Humans Rights and proceeds from the assumption that privacy is an inalienable right in itself. If privacy is an inalienable human right, then there can be no tradeoff of privacy against other rights such as property or security. Regardless of where one stands on these issues, it is undeniable that contemporary convictions about the value of privacy, whether as an instrumental or as an intrinsic right, are tangled up in what we will argue can be understood as the dichotomies and paradoxes of Western individualism. Our claim is that contemporary privacy discourse revolves not only around information but also around seemingly irresolvable conflicts, if not fundamental contradictions. We will argue that this leads to a "privacy paradox" in which privacy in both theory and practice tends to undermine and endanger much of what it is supposed to protect. Furthermore,

we will argue that it is for this very reason that privacy has become an "obligatory point of passage" from the industrial age to the digital age. Privacy can be seen as the form in which the autonomous, rational subject of Western modernity takes a last stand in the digital age.[5] Privacy forces us to think through the basic assumptions of modernity and to assess the implications of publicy and the informational self for concerns such as freedom, autonomy, and human dignity. Privacy, therefore, has become the "narrow gate" (Matthew 7:13) through which we must pass if we are to enter the promised land of the digital future. If we do not come to terms with privacy and the core concerns of privacy legislation and privacy theory, we will not be able to realize the full potential that a digital society promises.

In Part 3 we turn to the second word in our title, *Network Publicy Governance*, namely, "publicy." We make the daring and provocative proposal to replace the term "privacy" in all its theoretical and practical uses by the term "publicy." If the social actor is always a network constituted by information, and if information is more like a common good than private property, then the first step in moving beyond the privacy paradox might well lie in dropping the idea of privacy altogether. The informational self cannot be adequately conceptualized in terms of privacy. Stow Boyd has offered an interesting alternative. Boyd argues that digital network society has made transparency instead of secrecy the norm:

> There is a countervailing trend away from privacy and secrecy and toward openness and transparency, both in the corporate and government sectors. And on the web, we have had several major steps forward in social tools that suggest at least the outlines of a complement, or opposite, to privacy and secrecy: publicy. [...] The idea of publicy is no more than this: rather than concealing things, and limiting access to those explicitly invited, tools based on publicy default to things being open and with open access.[6]

Boyd goes on to explain what publicy consists of:

> From a publicy viewpoint...a person has social contracts within various online publics, and these are based on norms of behavior, not on layers of privacy. In these online publics, different sorts of personal status – sexual preferences, food choices,

5 | In a survey of 800 executives, the World Economic Forum (2015) singled out 21 technology shifts that will impact society in the near future. Among these are implantable technologies, digital presence, wearables, ubiquitous computing, supercomputing, data storage, IoT, smart homes and cities, big data, driverless cars, AI, robotics, blockchain, sharing economy, 3D printing, designer beings, and neurotechnology. In almost all cases privacy related concerns were listed as either hindrances or disadvantages.

6 | http://www.stoweboyd.com/post/765122581/secrecy-privacy-publicy

geographic location – exist to be shared with those that inhabit the publics. So, in this worldview, people are the union of a collection of social contracts, each of which is self-defined, and self-referential. [...] In this worldview, a person is a network of identities, each defined in the context of the form factor of a specific social public. There is no atomic personality, per se, just the assumption that people shift from one public self to another as needed.[7]

Contrary to the private self, the informational self derives its freedom, autonomy, and self-determination from rights that guarantee free expression, access to information, and free assembly. The tensions, if not antagonisms, between rights to privacy on the one side and rights to free expression on the other are not new. The advent of the digital age casts a new light upon this well-known controversy by focusing on information. If individuals are defined by information, it becomes more difficult to maintain the bounded, pre-social character of subjectivity. The default condition of human existence becomes publicy and not privacy.

The advent of publicy as the default condition of human existence need not signal the rise of a digital communitarianism or the demise of Western respect for the individual in favor of collectives such as family, clan, class, or state. We need to move beyond the sterile opposition of individual and society. Freedom, autonomy, and dignity are realized in communication and not before or outside of communicative action. Modern social theories of both systemic (Luhmann) and action-theoretical (Habermas) provenience have come to locate the foundations of the human person as well as society in communication. Legal philosophy formulates this view in rights to free expression and free assembly. Contrary to what privacy advocates claim, it is not the right to be left alone, but the right to have access to information, to create information, and to distribute it that lies at the basis of a democratic society. Speaking out makes a difference. Secrecy doesn't change anything. Paradoxically, privacy supports the injustices of the status quo that it is supposed to mitigate. Publicy on the contrary, demands that the right to speak must be protected and even actively enabled. What publicy emphasizes is that the informational self is essentially participative.

Characterizing the informational self in terms of publicy does not mean simply trying to transform natural persons into juridical persons. The self, whether natural or juridical, is not first and foremost a bounded individual who somehow enters into relations, whether cognitive, volitional, or emotional, beyond its borders. The informational self is constituted by associations, not only with others but also with non-humans. Associations are always mutually constituted by all actors involved in a network and cannot be dictated top down.

7 | http://www.stoweboyd.com/post/797752290/the-decade-of-publicy

Traditional metaphors of subjectivity and identity as something internal, as an internal vision, the eye of the mind, as free will and decision, or as emotion and desire are replaced by metaphors such as listening, negotiating, associating, and cooperating. The Cartesian ego and the autonomous rational subject of Western modernity must painfully acknowledge that cognition, action, and identity are distributed among many different voices and programs of action. This raises the question of how publicy is regulated. How does the mind keep its house in order if it is not its own independent and individual ruler? In the place of concepts and assumptions of immediacy, the universality of reason, and self-government (autonomy) which ground not only our understanding of subjectivity, but also privacy rights and regulations, publicy regulation must be conceived of as participatory, decentralized, distributed, and collaborative. Whereas it was possible in modernity to understand social order as based on the internal rationality of Cartesian egos and the external rationality of contracts and law, once the self has become information this no longer works. Publicy is the unique mode of human existence that can be described neither as an individual nor as a society in the modern senses of these terms. Neither autonomous rationality for the individual nor the social contract for society can account adequately for publicy. What kind of order does publicy have? We argue that understanding the default condition of the informational self as publicy lays the foundation for reconceptualizing not only subjectivity but also social order. This opens up the possibility of framing the legitimate concerns behind privacy regulation, data protection, and ideals of informational self-determination in a new way. We propose reformulating the problem of human self-understanding and social order in terms of *network governance* instead of (self)government.

The third term in the title of this book, *Network Publicy Governance*, namely, "governance." In Part 4 we turn to the question of regulating publicy. Doing away with the autonomous rational subject of humanism creates a vacuum with regard to the source of order. When the "rationality" of isolated individuals no longer bridges the gap between the one and the many, and when the social contract, as well as the representative government arising from it, no longer suffice to bring order into the global socio-sphere, where does order come from? How is the chaos of many-to-many communication to be channeled and ordered? The default condition of the informational self is publicy, that is, the condition of existing as information when information is neither private nor public. This raises the question of sovereignty and regulatory power as well as regulatory legitimation with regard to information. Information "belongs" to the network and the network is, therefore, the actor. Modernity located the source of order within universal reason which individuals possess and reason's collectively binding expression in law. Traditional discussions of either individual or collective regulatory power reflect this modern Western

understanding of the individual and society. They are bound up with the forms of social order typical of modern industrial society, that is, Hobbesian Leviathans and Weberian bureaucracies, with an occasional reference to chaotic revolution. The traditional term for describing social order is "government." Merriam-Webster defines government as "authoritative direction or control." This is what the ego does within the mind as well as what the king or president does within the state. It would not be an exaggeration to claim that government in one form or another has been the dominant form of social order, at least for large populations, for the greater part of human history. In the modern period, however, government was understood largely in opposition to another organizing force, the market. Government was often understood as a necessary correction of the inadequacies of market organization, whereas the market symbolized individual freedom. In this tradition, there are only two models of social order, either markets or hierarchies. Practical politics, as well as humanist ideology, was and for the most part still is divided into either "right" or "left" or a mixture of the two. During the entire modern era, there was and for the most part still is no third alternative. This is where governance comes in.

Networks are neither markets nor hierarchies, nor a mixture of the two, but a different form of order. Although networks have always been with us, as a consequence of the digital transformation networks have come to the fore. Castells has pointed out that networks are not new. "What is new is the microelectronics-based, networking technologies that provide new capabilities to an old form of social organization" (2005: 4). The digital transformation makes global networked organizations possible. Following the slogan, "governance without government" (Rosenau/Czempiel 1992), new decentralized, non-hierarchical, collaborative, and distributed forms of regulation typical of networks have become central topics in almost all areas of today's world. Of course, even in a network society, people must accomplish certain tasks and solve certain problems to make cooperative action possible. Goals must be set, stakeholders must be identified, roles and responsibilities must be assigned, processes must be designed, and compliance and controlling must be defined and implemented. Governance does not change the basic tasks of organizing cooperative action, but it attempts to solve them on a different basis and in a different way than does bureaucratic government.

Governance is a term with many different but associated meanings and has become the focus of discussions in various disciplines from international studies to policy administration, organization theory, and sociology. Governance is a matter of a complex overlapping of rules of many different kinds based on many different sources and not merely formal laws instituted and enforced by centralized authorities. What governance studies in many areas have shown is that both hierarchical and market models are inadequate when it comes to

understanding how heterogeneous networks are regulated. Actors of many different kinds play constructive roles in shaping regulatory measures outside of and beyond formal, state-sanctioned laws. Neoinstitutionalist economics, for example, has focused on various forms of governance as ways of regulating that are based neither on markets nor hierarchies. Decades of empirical work have shown the limitations of traditional economic models of either private property regulated by a free market or government-owned property regulated by hierarchies. Instead, what has become increasingly important in economic theory and actual practice are "self-organized resource governance regimes" (Ostrom 2000: 138). The public/private dichotomy, whether applied to resources or actors, has become increasingly dysfunctional. This is above all the case when actors are seen as networks constituted by information.

Information is neither exclusively private nor exclusively public. Informational selves and the publicy networks in which they exist do not dissolve into chaos when markets and hierarchies become dysfunctional. Governance steps in where market exchange or governmental command and control fail. Problems of regulating flows of personal information are therefore not adequately conceptualized either by privacy or by government protections and restrictions. *Informational self-determination is a problem of governance and not of government*. We propose using the resources of contemporary governance discourse interpreted from the point of view of actor-network theory and the affordances of digital technologies to describe network publicy governance. We argue that successful strategies of common-pool resource governance,[8] such as clear identities, proportionate equivalence of benefits and costs, collective-choice arrangements, rights to self-organize and to establish flexible and locally appropriate conflict resolution mechanisms, as well as open and flexible boundaries can be theoretically anchored in a general theory of *governance by design*.

Based upon ANT, we propose a *reconstruction of governance theory* that focuses on processes and not on structure. Networks, as opposed to traditional organizations, are not ordered by governing structures, but by governance processes. Each actor in a network, whether human or nonhuman, has a "voice" of its own, while at the same time contributing with this voice to building a collective capable of cooperative action. This implies that networks regulate themselves by taking account of all possible voices or actors that could claim to contribute to the network. This process of *taking account of* allows for new *stakeholders* to be integrated into the network, while at the same time raising the question of which stakeholders play decisive roles. Since not all stakeholders are equally important, *prioritizing* the relative importance of different actors and *institutionalizing* relatively stable roles and identities are

8 | See for example. Ostrom (1990); Wilson/Ostrom/Cox (2013).

important regulatory processes. Institutionalized actors tend to be constituted by many links and associations so that if one tries to change any single link, one has to change them all. This characteristic of network governance is the basis for what is often called "structure," that is, repeatable, relatively fixed identities and processes. Although institutionalizing reduces the complexity of networks and thereby excludes certain actors, roles, and processes, it does not eliminate flexibility. Unlike traditional organizations, the boundaries of networks are not constitutive, but merely regulative. Networks exclude not to become networks but to practically deal with a particular problem or pursue a specific goal. This is the *localizing* function of network regulation. Networks reduce the complexity of many different and diverging possible activities by focusing on a local problem or goal.

Localizing creates a limited and goal-directed program of action or what can be called the trajectory of a network. The effects of localizing are well-known in social theory and have been described in a variety of ways. The description of society as consisting of different domains or sub-systems, for example, business, politics, science, education, religion, and art and of different levels such as the micro, meso, and macro can be seen from the network perspective as the results of localizing. Furthermore, Goffman's famous dramaturgical account of social interaction in terms of actors, scripts, and frames can be understood as a description of the network governance process of localizing. In terms of privacy theory, Nissenbaum's (2004) well-known notion of "contextual integrity" makes privacy expectations dependent on social contexts. Contextual definitions, however, are not merely given. In a quickly changing world, social contexts are no longer guaranteed by tradition. Neither can they be derived from fundamental rights nor dictated by governments. Local contexts must be constructed and for this reason there is no guarantee that privacy always plays an important role or perhaps any role at all. This leads directly to publicy. Publicy means that it is the localizing function of network governance that defines the context of information use as well as the relevant identities of the actors. Publicy, however, is not merely local. Social contexts are always linked up to others in many different ways leading on up to a global dimension. The answer to the question, who am I? is never merely local. The fundamental openness and the flexibility of networks prevent any local regime from becoming a closed system with uncontestable boundaries. Localizing, therefore, implies also *globalizing* and both are important network governance processes. Globalizing means that localized networks are always in many ways linked to each other and thus integrated into a global dimension, a global "socio-sphere" or what is usually called a "world." Localizing is only possible against an open horizon of a global collective, just as every local situation is part of the world and affected by global events. Finally, network governance also includes processes of *balancing the*

powers of closure and openness, the local and the global, the institutional and the unexpected.

The processes of network governance derived from ANT become interesting for a theory of network *publicy* governance when the affordances of digital information and communication technologies are taken into account. When digital technologies become our most significant nonhuman others in the construction of information, social order, and ourselves, then the processes of network governance follow *network norms*. The governance process of *taking account of* possible actors is manifested as *connectivity* and *flow*. Every actor or device added to the network brings new information, new "voices" into the collective. Every actor or device, be it ever so inconspicuous and of apparently only local importance, gains access to global networks and participates in global flows of information. Smartphones, smart homes, smart cities, smart automobiles, smart energy, smart communication and transportation networks, smart logistics, industry 4.0, data-driven organizations, personalized products and services, machine learning, data science, and much more all testify to the connective imperative. What makes these connections "smart" – and also threatening – is, of course, the flows of information they enable.

Network governance processes of *producing and prioritizing stakeholders* are influenced by the network norms of *communication* and *participation*. Producing stakeholders under the affordances of ICTs is much more distributed and complex than in hierarchical government, but also much less chaotic and opportunistic than in free markets. In the global network society, bottom-up, collaborative, and self-organizing practices of prioritizing stakeholders and institutionalizing roles, identities, and processes are more effective than traditional forms of regulation. In addition to this, the effect of digital affordances has been to create many more stakeholders in all kinds of networks than were possible under the conditions of informational scarcity and one-to-many communication. This wide distribution of stakeholders has been termed "participatory culture." The digital transformation has placed the means of the production of information into everyone's hands. It has empowered consumers to become prosumers not only in business, but also in education, healthcare, social service administration, and politics. The advent of many-to-many communication in the digital age has brought the participatory potential of networks to the fore.

Networks not only produce stakeholders in new ways, but they also set priorities and institutionalize roles, identities, and processes on the basis of the norms of *transparency* and *authenticity*. If publicy and not privacy is the default condition, it becomes increasingly costly to attempt to set agendas and maintain political or commercial advantages by means of secrecy. In the digital age, knowledge is only then power, when it is shared and used collectively. This, in turn, requires that the sources, the quality, and the intended purposes of

information are transparent and that actors do not misrepresent themselves. Networks operate on the basis of trust. Trust is based on transparency and authenticity. Privacy, on the contrary, is based on mistrust and obfuscation. Not knowing who one is dealing with, not knowing what information is valid, and not knowing what information is intended to be used for make organizations inefficient, costly, and at least in the long run bound to fail. When the norms of transparency and authenticity are not followed, the wrong stakeholders are prioritized and others who should not are excluded. Inadequate structures become institutionalized and are no longer questioned or revised.

Finally, the norm of *flexibility* takes network governance a step further and influences how processes of *localizing/globalizing* and the *balancing of openness and closure* are implemented. Large networks encourage the autonomy and self-organizing capabilities of local networks so that they can adapt to unforeseen problems and take advantage of unique and unexpected opportunities. This is a problem that systems theory clearly recognized but could not solve. Systems find themselves in the paradoxical situation of being able to reduce environmental complexity only by increasing internal complexity, which creates ever greater strains on system organization.[9] There is an inherent tension in the primary purpose of systems to reduce complexity on the one hand and on the other hand the necessity of having to constantly increase internal complexity to maintain viability in the face of an ever more complex environment. Network publicy governance deals with complexity in an entirely different way. When networks that are influenced by the affordances of ICTs localize programs of action against a global horizon of possible network extensions they realize a flexibility or adaptability for which cut-throat evolutionist theories have to pay much too high a price. In the Darwinian world, it is a matter of either change or die; whereby radical change amounts to the same as death. Network publicy governance, on the contrary, follows the norm of flexibility by means of channeling the opposing forces of *localizing* and *globalizing* and *taking account of* and *institutionalizing/excluding* on the basis of the normative affordances of connectivity, flow, participation, communication, transparency, and authenticity.

From the point of view of network publicy governance, many of the problems that characterize the conflict between privacy protection and data exploitation simply don't arise. Information is from the outset neither private nor public. There is no inherent violation of rights when so-called personal information is used to create value since not only information but also value is defined as belonging to the network and therefore to be regulated by the network's own governance processes. Misuse of information in all its forms remains just

9 | See Ashby's famous "law of requisite variety" (Ashby 1956), as well as the vast literature on systemic management which attempts to deal with this problem.

what it is, misuse that must be prevented and sanctioned. Based on a theory of information, a critique of the basic assumptions of privacy discourse, a vision of the human as an informational self, as well as an ANT-inspired reconstruction of governance theory, we propose a theory of governance not as external regulation but as an internal and ongoing *design process*. This demands a new narrative, the narrative of the clever designer who carefully takes account of all voices and who ensures communication and participation instead of the heroic but tragic individual of modern humanism.

This book builds upon but does not presuppose, earlier work that we have done on the meaning and effects of the digital transformation. In *Interpreting Networks* (2014) we examined how the order of knowledge has changed due to the affordances of digital technologies. In *Organizing Networks* (2016) we looked at what digital transformation means for the order of society. In this book, we raise the question of what living in a post-humanist, global network society means for human self-understanding. It is perhaps in these three areas, knowledge, society, and human existence that the digital revolution has most dramatically transformed the world we live in. The guiding light in these investigations and thought experiments has been actor-network theory (ANT). We chose ANT because we believe that its provocative inclusion of nonhumans in society and its programmatically non-modern conceptual repertoire are best suited to understand the world we are entering into, a world in which, as Floridi puts it, humans must share the attribute of intelligence with machines. If the "fourth revolution" is indeed a revolution, then much has changed and will continue to change in the ways in which we interact with information, construct social order, and experience ourselves as actors and creators of meaning. We are well aware that these changes will most probably not be foreseeable and calculable. They will constantly surprise us. The conceptual tools we use today will undoubtedly prove inadequate in the future. Nonetheless, we hope with this book to contribute to a constructive and heuristically useful discussion of our common future.