2014

# Location Data, Purpose Binding and Contextual Integrity: What's the Message

Mireille Hildebrandt, *Radboud University Nijmegen*

# Location Data, Purpose Binding and Contextual Integrity

# What's the Message?·

**Mireille Hildebrandt**

***Abstract*** This chapter investigates the issue of the proliferation of location data in the light of the ethical concept of contextual integrity and the legal concept of purpose binding. This involves an investigation of both concepts as side constraints on the free flow of information, entailing a balancing act between the civil liberties of individual citizens and the free flow of information. To tackle the issue the chapter starts from Floridi's proposition that 'communication means exchanging messages. So even the most elementary act of communication involves four elements: a sender, a receiver, a message, and a referent of the message' and his subsequent proposal that informational privacy can be described as 'the freedom from being the referent of a message'. After discussing the current environment of messaging in terms of Big Data Space and the Onli*f*e World, the chapter develops a more detailed definition for the right to informational *location* privacy. The road to this more detailed definition allows to highlight the balancing act inherent in both contextual integrity and purpose binding, and shows that the most salient challenge for such balancing acts is not – only - that Big Data Space and the Onli*f*e World turn contexts into moving targets. More importantly, the context of economic markets tends to colonize the framing of other contexts, thus also disrupting the protection offered by purpose binding. To safeguard informational privacy we need to engage in new types of boundary work between the contexts of e.g. health, politics, religion, work on the one hand, and the context of economic markets on the other. This ardent task should enable us to sustain legitimate expectations of what location messages are appropriate as well as lawful in a particular context.

· The research for this chapter was done in the context of the interdisciplinary research project on 'Contextual privacy and the proliferation of location data', funded by the Flemish Science Policy Agency (FWO), which entails a collaboration between computer engineers and lawyers from Vrije Universiteit Brussel and Katholieke Universiteit Leuven. I want to thank my co-researchers on the project for their many insights: Claudia Diaz, Laura Tielemans and Michael Herrmann. I also want to thank Helen Nissenbaum and Tal Zarsky for their comments on an earlier version of the paper and all participants to the 'Privacy Workshop: From Theory to Practice' at Haifa University in December 2013.

## 1. Introduction: What's the Message?

Luciano Floridi has defined communication as 'exchanging messages'.[1] In this chapter I want to investigate whether this – cybernetic – starting point helps in understanding what EU legislation terms as 'data processing' and what Helen Nissenbaum has called 'flows of information'.[2] More specifically, I will investigate how it helps to understand the implications of the proliferation of location data for the right of informational privacy. Obviously, the sending and receiving of messages introduces actors that are not necessarily implied in the concept of data processing. Within EU jurisdiction data processing can refer to computational operations within computing systems, such as storing and retrieving of data or further manipulations such as data mining, that cannot be described as the sending of messages.[3] Even the collection of data is not necessarily a matter of senders and receivers, since the receiver of the data may collect it without any deliberate effort on the side of the data-holder. In fact, the data that was collected may have been 'manufactured' by the receiver, for instance in the case of clickstream behaviours or other types of machine-readable behavioural data. Thinking in terms of messaging clarifies this by highlighting that the data was not sent but taken, with our without consent. Phrasing the issue of informational privacy in terms messages also raises the question of what insights are gained (and lost) if we understand machine-to-machine communications as the exchange of messages instead of merely the exchange of data. The notion of a message seems to entail more than data, notably a direction and some form of – mindless or mindful - intent. This chapter aims to figure out how speaking of messages instead of data enhances or reduces our understanding of what is at stake with the proliferation of location data.

As Floridi notes, 'even the most elementary act of communication involves four elements: a sender, a receiver, a message, and a referent of the message'.[4] This highlights the flow of messages between senders and receivers, thus qualifying the notion of information flows in terms of points of departure and arrival and specifying the 'aboutness' of the information in terms of a referent (rather then, for instance, an owner of the data). In respect of the proliferation of location data, building on Floridi,[5] we can now formulate four fundamental rights and freedoms that concern location data in terms of the exchange of

[1] See the introduction to this volume [or the Fiesole Workshop].
[2] On cybernetics Wiener (1948). On EU data protection De Hert and Gutwirth (2006). On contextual integrity Nissenbaum (2010).
[3] In intra-machine data processing the actors could be those ordering or operating the processing; in the EU legal framework these actors are defined as data controller and data processor. From the perspective of cybernetics the actors would be the machines (software and/or device) that sends the message, referring to a mindless form of agency.
[4] See n 1.
[5] See n 1.

messages: (1) freedom of speech concerns the right to send messages from whatever location to whatever location, including the right not to be located when exercising freedom of speech, (2) freedom of information concerns the right to receive messages from whatever location to whatever location, including the right not to be located when exercising freedom of information, (3) communication security concerns the right to protection from unwanted access to one's location data, manipulation of one's location data or destruction of one's location data (CIA) and (4) the right to informational location privacy concerns the freedom from the referent's location data being shared without consent or necessity.[6] Though all these rights and freedoms can thus be translated into location-data-relevant formulations, this chapter will limit itself to informational privacy in the broad sense of what the OECD has called the 'fair information principles (or policies)' and what is defined as 'data protection' within the European Union (EU). In saying that informational privacy refers to the requirement that information is shared on the basis of either consent or necessity I hope to catch both purpose binding and contextual integrity as normative frameworks that delimit (1) data processing, (2) flows of information, (3) the sending of messages.

In the following sections I will first discuss the informational location privacy in the context of Big Data Space, followed by the introduction of three types of data with a large impact on autonomy, identity and privacy: volunteered, observed and inferred data. This results in articulating informational location privacy as relating to 'raw', networked and 'processed' data. The impact of this data will be further explained and developed by investigating the consequences of various types of location messages in the context of the so-called Onli*f*e World, challenging traditional (modern) notions of autonomy,[7] identity and privacy. All this should create the middle ground for the sections on the ethical concept of contextual integrity, notably the contextual privacy decision heuristic, and the legal obligation of purpose binding as exemplified in the EU framework of data protection. Finally then, I will evaluate how framing informational location privacy in terms of messaging helps to understand to what extent contextual integrity and purpose binding are side constraints or require a balancing act.

[6] Communication security is the odd one out, since it is not a fundamental right. One can, however, easily relate it to the foundational tasks of the state in securing critical infrastructure, and safety and/or relate it to the confidentiality of communication that is at stake in the right to informational privacy.
[7] Obviously modernity constitutes a tradition, despite the fact that it is often framed as liberating itself from any type of tradition.

## 2. A cybernetic starting point: Location data in *Big Data Space*

The idea that an act of communication can be defined as the exchange of messages takes its clue from Wiener's theory of cybernetics. Wiener connected the notion of communication with that of control, claiming that the exchange of messages is meant to give agents a certain measure of control over their environment. He formulated his theory to explain communication between machines, explicitly defining human persons as machines. In doing so, he hoped to enhance scientific understanding of human-to-human, human-to-machine and machine-to-machine communication. Though we need not agree that human persons are machines, it makes sense to follow up on Wiener's semantics for the simple reason that our online and offline environments are increasingly constructed and 'animated' by interactive computing networks, built on the semantic assumptions of cybernetics.[8] By adopting the idea that communication is a matter of messages sent and received, with a content that refers to something outside of the message, we can for instance flesh out to what extent human persons are indeed messaging machines and, if so, to what extent their messages differ from those of other messaging machines (plants, animals, robots, artificial agents).

Beresford and Stafano have defined location privacy as 'the ability to prevent other parties from learning one's current or past location'.[9] Based on Floridi, we can translate this as 'the freedom from the location of the referent, the sender or the receiver of a message being shared'. This highlights the idea that privacy is a liberty (*freedom from sharing*) rather than an issue of control (*the freedom not to share*). Obviously, Beresford and Stafano emphasize the aspect of self-determination in the narrow sense of control (the freedom to share or not to share). However, defining informational location privacy in this way is too absolute. We need to take into account that informational privacy does not equate with hiding per se, but with the *capability* to hide or remain hidden *if there is no necessity or consent for sharing information*. Note that the EU legal framework is focused on discrete *personal data*, whereas my definition is focused on a *data flow*.[10] Similarly, as noted above, the EU legal framework is focused on the *processing* of personal data, which includes all kinds of operations such as the recording, storing, retrieving, computing, deleting, pseudonomysing or anonymising of personal data, whereas my definition is focused on the *sending of messages containing* personal data. The advantage of thinking in terms of data flows and messages

[8] With a semantic assumption I mean an implicit understanding of the meaning of the foundational concepts of cybernetics. The fact that cybernetics is more interested in syntaxis than in semantics obviously does not entail that its own vocabulary is devoid of meaning. On the history of cybernetics Hayles (1999).
[9] Beresford and (Stajano 2003).
[10] This is also one of the important advantages of Nissenbaum's understanding of contextual integrity in terms of information flows, see section 5 below.

could be that it gives prominence to the dynamic and interactive character of exchanges of location data. This does not imply that the processing of location data that is performed by computing systems is of no relevance, but it allows to discriminate between intra-machine processing on the one hand and the exchanges of 'processed' location data between machines and humans on the other. Especially when specific decisions are taken on the basis of 'processed' location data, it is important to distinguish the processing from the exchange, and both from the decisions they nourish. In this chapter I will, therefor, use the term 'processed' location data as referring to location data that have been 'refined' by computing systems that use 'raw' location data as a resource for what some have called 'data derivatives'.[11] Because it is possible to infer location data from other data (e.g. from mobility patterns or energy usage behaviours), I will also use the term 'processed' location data for inferred location data. Though EU data protection law uses a broader definition of data processing, I want to discriminate between the first 'making' of the data and the various products 'made' by further processing of the initial data. This highlights the difference between 'raw' and 'inferred' location data on the one hand, and between 'raw' location data and inferences drawn from such location data about other aspects of an individual person on the other hand.

Before further exploring the particulars of location data in terms of a message, we need to discuss the environment in which all this communication takes place. To do this I will introduce two new terms: the first being *Big Data Space*, the second the *Onlife World*. Both terms highlight, first, the computational layers which constitute large parts of our environments, and, second, the hyperconnectivity of the emerging life world. Thirdly, they foreground the increasing entanglement of online and offline environments. In this section I will focus on the notion of Big Data Space, leaving the discussion of the *Onlife World* for section 4.

*Big Data Space* refers to the fact that the amount of available data enables new types of artificial intelligence, notably knowledge discovery in databases (KDD) and machine learning (ML). Paraphrasing Mayer-Schönberger & Cukier we could say that Big Data enables to do things that are not possible with 'small data'; Big Data introduces differences that make a difference,[12] though we may not yet be in the clear on what difference is crucial. *Big Data Space* also refers to the fact that databases are fused or matched, while the knowledge that is inferred can be stored, sold and re-used in other databases, thus generating a network of interconnected data servers, inference machines and virtual machines that

[11] The term 'data derivatives' was coined by Amoore (2011). With raw data I do not mean to suggest that 'data' is somehow 'out there', merely to be picked up. Digital data is always a translation from the flux of life and already incorporate specific assumptions about what experiences or observations qualify as what type of data. See Gitelman (2013).

[12] On these differences see Mayer-Schönberger and Cukier (2013), boyd and Crawford (2011), Hildebrandt (2013a).

constitute a complex, textured space with distributed access points.[13] To the extent that this space is connected with the Internet we can call it cyberspace, but since many interconnected computing systems are not connected with the Internet (various types of 'walled gardens' like the NSA and data brokers like Axciom or Experion) I will speak of *Big Data Space*, taking note of the fact that this is neither a homogeneous space nor a space that can be defined in purely spatial metaphors. *Big Data Space* is a timespace that synchronizes data exchanges, involves massive parallel processing, and challenges traditional notions of past and future. It combines an external memory for text, images, computing programs and real-time pattern recognition with a plethora of techniques for predictive analytics and feedback mechanisms. Other than the external memory constituted by written and printed text *Big Data Space* is radically dynamic and polymorphous, while its operations are informed by complexity, because they are, to some extent, recursive - due to the use of ML techniques that persistently *nourish on* and *reconfigure* the timespace of Big Data.

Taking into account that location data will often be situated in *Big Data Space* we must acknowledge that location data will often be 'processed' data and/or networked data. The latter is data that is or can easily be linked with other location data of the same person, of other persons, or with other types of data (e.g. purchasing data, energy usage data, video consumption data, education data, employment data). Informational location privacy should therefor include 'the freedom from networked and/or 'processed' location data being shared with others without consent or necessity'. Especially when decisions are taken about the referent, sender or receiver that are based on networked and/or 'processed' location data, achieving location privacy would imply that such data have been shared with informed consent or based on the necessity required by, for instance, EU data protection legislation. Note that location privacy is not about hiding or controlling one's location data, but about the conditions that must be met when location data and its derivatives is being shared. Note, also, that these conditions are not formulated as balancing acts but as side constraints; if they are not met the sharing is unlawful. That is why informational location privacy is a freedom: the freedom from unlawful sharing of 'processed' or networked location data. Such a formulation does not preclude that a justifiable interpretation of the side constraints may involve a balancing act, notably the proportionality test that is inherent in the condition of necessity.[14]

Lawyers will focus on location data that relate to an identified or identifiable natural person, because this constitutes 'personal data' (in the EU) or 'personally identifiable

[13] This also refers to cloud computing, which changes the scope, the security, the availability, accessibility, the distribution and the virtuality of the space of and for Big Data.
[14] See the last section of this chapter.

information' (PII, in the US).[15] However, 'processed' location data may consist of patterns or inferences that do not qualify as personal data, though they affect a person whose location data matches such 'processed' location data. This raises the issue of whether the concept of personal data or PII is salient or even adequate in addressing the notion of informational location privacy. In the next section we will follow the trail of the World Economic Forum (WEF) that has made the attempt of rethinking personal data in the era of Big Data Space, taking into account that the monetization of personal data is the driver for a number of business models. In distinguishing volunteered, observed and inferred data they propose to develop a more refined understanding of what is at stake in the era of Big Data, KDD and ML.

## 3. Three types of location data

The common sense on informational privacy seems strongly attached to the idea that personal data are owned by the person to whom they refer, leaving it up to her to decide to either share or hide them. The notion of ownership is confusing here, because it implies that we are talking about an exclusive right to a rivalrous good. A rivalrous good cannot be possessed by more than one person: once I take it from you, you don't have it anymore.[16] Personal data does not fit that category; it can easily be shared with a number of people without taking it away from whoever it refers to. In fact, many 'processed' data were never in the possession or even awareness of their referent. Indeed the whole idea of personal data is to share information about oneself, to allow others to identity and address one. If you get to know my name you may have little use for it if everyone else – including me – is forced to forget it (this would be the case if it were a rivalrous good). The fact that personal data is often discussed in terms of ownership is of course related to the fact that people feel strongly about the knowledge and information that concerns them, which they believe to *belong to* them. This leads people to claim that they are somehow *entitled* to it. Such entitlement, however, does not imply exclusiveness. Different legal subjects can have different types of entitlements to the same data. Take, for example, energy usage data. If it refers to a particular household with identifiable users, energy usage data is personal data for those that are capable of linking the data to the identity of the user. The energy supplier that has a contract with the user will need

[15] PII and personal data are defined slightly differently and the legal effect of a data being qualified as PII in the US or as personal data in the EU differs.
[16] Joint possession of the same good is possible, but that is not the point here. On property of personal data see e.g. Prins (2006) and Purtova (2012).

subscription data to prepare the bill and location data to supply the energy. This means that the user has data protection rights towards the supplier, while the supplier has the right to require, store and retrieve the data for the purposes of energy supply and billing. Obviously, based on energy usage patterns, the supplier could *infer location data* for the members of the household based on their use of electricity or gas. To the extent that the supplier has no need for such data, a supplier that is active within the EU jurisdiction is not allowed to process them. The purpose binding principle stipulates that personal data may only be processed for an explicit, specific and legitimate purpose and may not be reused for an incompatible purpose.[17] So, informational location privacy here means that energy suppliers should refrain from sharing 'processed' location data of their subscribers.

Recently, the WEF has been discussing the tensions between the interests of senders, referents, recipients, users and processors of data in terms of volunteered, observed and inferred data.[18] This may enable a more precise understanding of what is at stake with the proliferation of location data. *Volunteered data* are the data that people deliberately provide, and often also 'make':[19] pictures or text posted on Facebook, emails sent to friends or colleagues, credit card details or an address for the delivery of a book. Volunteered data are part of a message, sent by the referent of the message to a particular or even to an unlimited audience (e.g. in the case of a publicly accessible blog). Social Networking Sites (SNSs) such as Foursquare enable people to share their location data with friends, to make themselves visible and reachable in a certain location. Users of Foursquare basically *have* messages *sent* on their whereabouts. However, Foursquare may decide to retain the content of the message and its metadata in order to sell such data to providers of location-based services or personalized advertising. This is not because the user had sent a message to Foursquare, but because Foursquare *observed* the location and 'datafied' it to enhance its business model.[20] Datafication refers to the process of translating the flux of life into discrete, machine-readable data points. The message sent by the user was intended for her friends; the SNS was merely the enabler. However, as we all know, the enabler makes its money by using the behavioural data (of which location is but one) to pay for its operations and to make a profit. So, the

[17] See art. 6 of the Data Protection Directive (DPD): D 95/46/EC and art. 7 of the draft General Data Protection Regulation (dGDPR). To supply energy and to address the bill, the supplier must have the location of the household; it is, however, not allowed to infer and use the location of individual persons within the household for other purposes than energy supply and billing.

[18] World Economc Forum (2011, 2012).

[19] To the extent that such data form a 'work' by an 'author' they generate copyright.

[20] Datafication will also generate copyright or other intellectual rights, but now on the side of the service provider (the observer) of the data. Whether this is the case depends on the jurisdiction and the nature of the process of dataficiation. For instance, a patent on the software that creates the data may be copyrighted or patented, the database that is used to store the data may entail a sui generis IP right or a copyright, the data mining software may be patented or subject to copyright. An interesting question is whether the data itself is the object of an IP right on the side of the 'datafabricator' or whether it can claim be subject to protection as a trade secret.

location data is both volunteered (in regard the friends) and observed (by the SNS). It is important to acknowledge that whether a data is volunteered or observed depends on the relationship between sender and receiver and not on the data itself; this implies that the same data may be volunteered within the relationship between the user of an SNS and her friends, but observed within the relationship between the user and the SNS provider. On many occasions the entities that collect behavioural data do not even have a relationship with the person whose behaviours are datafied. Advertising networks such as Double Click (now Google) and services such as Google Analytics (guess what, also Google) are employed by web portals, web shops, and a host of online service providers (whether public or private), who observe and 'process' online behavioural data on behalf of whoever wants to 'improve the user experience' or their own profit (which is assumed by some to coincide). For instance, websites often employ so-called A/B research design to personalize their interface to the observed or inferred location of the visitor, e.g. by adapting the language, the currency and – of course – the price of the services that are offered. The relationship between the user of the SNS and those third parties can be qualified as eavesdropping, if we think in terms of messaging.

Observed data are the measurable behaviours of 'onliners' and 'offliners' that can somehow be datified: click stream behaviours online, transaction behaviours that involve loyalty cards, public transport behaviours read from the public transport smartcards, health related behaviours that feed into remote healthcare systems, traffic data of telecom end-users and the more. These data are not necessarily volunteered: they need not be deliberately provided or fabricated by the person whose behaviours they refer to. They are 'made', 'constructed', 'read', 'measured' by a plethora of computational machines that are increasingly adapting online and offline (our Onli*f*e) environments to suit inferred preferences of the user (or of whoever pays for them). *Big Data Space* is stuffed with observed data; i.e. with datafied behaviours of individuals, crowds, eye-movements, weather conditions, products (life cycle management), skin conditions, eye-movements, gait, financial transactions, security vulnerabilities, blood composition, whatever. Critical infrastructure is increasingly dependent on such observed data (cf. the smart grid) and most business models cannot gain competitive advantage without them. Even our governments display a firm belief in the added value of massive datafication (think NSA, but also China or Europe – each in its own way, with its own justifications). Location is an easy target for datafication in the era of smartphones and other mobile devices, products enhanced with radio frequency identification (RFID) tags, CCTV camera's and other gear that enables to locate an individual person in timespace. Apart from location based services (LBSs) most of the datafication will concern observed location data.

The added value of volunteered or observed location data is not so much in the growing aggregation of discrete data points, even if these are traded and monetised in the high frequency markets of advertising space or stored for as yet unforeseen future re-use. The added value is in the inferences. Here we encounter the most interesting privacy paradox. Volunteered and observed data will often be personal data (insofar as they relate to an identifiable person), whereas inferred data concerns patterns and correlations at a higher level of (statistical) abstraction that cannot be qualified as personal data. However, it is precisely these patterns that form the trove against which our data points are matched and correlated. The inferred data are the gold that is mined from the 'raw' (volunteered or observed) and the 'processed' or networked location data. Not only do these inferred data have a more permanent and transformative impact in the Onli*f*e World, they lack the protection available for 'unprocessed' data while they will often enjoy protection as part of the trade secret or intellectual property rights of those who invested in producing them.[21]

Volunteered data clearly constitutes messages, intended for one or more specific addressees. It may, however, be received by other parties that observe such data to enhance their business case. Though observed data may also be defined as constituting a message, it is not entirely clear what is the meaning of a 'sender' in that case. On top of that we need an extra term to distinguish the addressee of the message from the receiver (though they may coincide). One way of analysing observed data as a message is to qualify the machine, the software and/or the hardware) that enables observation, as the sender. Another way would be to qualify the receiver as the sender to the extent that the receiver has initiated the process of having the data sent to its own processing engines (e.g. by means of cookies, or browser fingerprinting). Finally, one could simply say that the data is taken instead of being sent; by highlighting that no message was sent while data was still captured the difference with volunteered data stands out. To describe observed data in terms of messaging we seem to require the concept of intent, raising two further issues: first, does sending imply intent?, and, second, should we accept the notion of 'mindless' intent to refer to machine-to-machine exchanges of data? I will leave this in the middle for now, and conclude that whereas volunteered and observed data can both be understood as messages, inferred data is another matter. Data derivatives may form the content of a message, but – like other types of 'processed' and networked data – they do not necessarily involve a data exchange. In the next section I will discuss volunteered, observed and inferred location data in the context of the emerging Onli*f*e World, hoping to flesh out how the messaging of 'raw', networked and 'processed' data is impacting everyday life in this new 'Onli*f*e World'. This should create a

[21] See e.g. recital 42 of the current Data Protection Directive D 95/46/EC.

middle ground to discuss informational location privacy in terms of contextual integrity and in terms of purpose binding.

## 4. Beyond cybernetics: location data in the *Onlife* world

The 'Onli*f*e World' is a concept developed by the Onli*f*e Initiative, a group of philosophers, social scientists and researchers of artificial intelligence, brought together by Nicole Dewandre and Luciano Floridi.[22] The aim has been to contribute to the reengineering of current conceptual frameworks. Though concepts cannot be 'fixed' in a mechanical way, they can be in need of mending or even reinvention. It should be clear that traditional (i.e. modern) conceptions of self, mind and society have been disrupted by the rapid transformations brought about by game changers such as the mobile smartphone, algorithmic search engines and online social networking sites. In speaking of conceptual reengineering we refer, for instance, to the notion of philosophical engineering as used by one of the founding fathers of the world wide web, Tim Berners-Lee, who exclaimed in an email exchange: '(…) we are not analyzing a world, we are building it. We are not experimental philosophers, we are philosophical engineers.'[23] I read this as a call for awareness, addressing those who engineer the information and communication infrastructures of our current era, reminding them of the constitutive impact of their building, crafting and tinkering on what can make or break us as individuals, as societies, and as increasingly onli*f*e hybrids. For me, the concept of an Onli*f*e World tweaks the increasingly inadequate notions of online and offline, while focusing on what this means for our 'lifeworld', in both the everyday and the phenomenological sense of the term.[24] The Onli*f*e Initiative thus admits that some of the foundational concepts of modernity are inadequate, insofar as they are incapable of coping with the relational nature of the self and the increasing heteronomy of human-machine relationships. The intuition that triggers the Initiative is that both hyperconnectivity and invisible computational decision

[22] See <https://ec.europa.eu/digital-agenda/en/onlife-initiative>. I am one of those 'gathered' by the initiators and the many in-depth discussions have inspired my own thinking, especially complementing my research into the computational turn with more focused attention to the hyperconnectivity of the emerging lifeworld.

[23] See <http://lists.w3.org/Archives/Public/www-tag/2003Jul/0158.html>; Hildebrandt (2013b): 235. Conceptual engineering can also be understood as derived from Carnap's logical positivism, which aimed for an '*unphilosophical philosophy*, (…) building up from clear, technical, first principles. (…) striving for 'a "modern" way of life, (…) grounded on a vision of the machine age' Galison (1990): 750. My own link with philosophical engineering hooks up with Tim Berners-Lee's exclamation that engineers are constructing and shaping our lifeworld. I take a pragmatic and phenomenological perspective, cf. Ihde (2008).

[24] Husserl (1970). Ihde (1990)

systems challenge vested notions of, first, human autonomy; second, Westphalian sovereignty and; third, the common sense difference between mind and matter. *Big Data Space* enables pattern-recognition that allows for subliminal manipulations of consumer preferences that correlate with 'raw', networked and 'processed' location data, thus challenging the assumption of human autonomy; it sparkles cross-border access to 'raw' and 'processed' location data by law enforcement and foreign intelligence services, thus challenging the assumptions of internal and external sovereignty; and, finally, *Big Data Space* enables computing systems to develop of a mind of their own – acting on the feedback they infer from their environments, thus challenging the experiential duality of passive matter versus active mind. The latter is especially relevant with regard to location data, since smart environments may confront individual persons with anticipations of their 'whenwhereabouts'.

At the same time, we are confronted with the experience of hyperconnectivity – across the extended timespace of messaging services such as e.g. skype, sms, WhatsApp, email, and across the hyperlinked virtual space of the world wide web, the page rank algorithms of search engines and the scaling of interrelationships in the realms of social networking sites. This entangles us with the network effect of complex non-linear relationships of cause and effect. A fundamental unpredictability has surfaced, leaving us with a sense of uncertainty and liquidity; presenting a trove of surprising opportunities (novel business models, scientific discovery, risk management) and devastating misfortunes (e.g. the financial crisis). Such unpredictability changes the meaning of meaning, disrupting the foreseeability of the consequences of our actions, thus reducing or even transforming our understanding of human autonomy and undoing the assumptions of national and international jurisdiction, while making us dependent on the technological infrastructures that mediate and constitute our environment.

The philosophical concept of the lifeworld, coined by Husserl and further developed by phenomenologists such as e.g. Merleau-Ponty, Ricoeur, Varela and Ihde,[25] refers to the way we perceive, cognize and co-constitute our environment, while at the same time configuring our sense of self and society. It regards the way we are 'at home' in the world, navigating familiar surroundings, anticipating the habits and habitations of our fellows and of the institutions or social structures that co-determine our consolidated expectations. Philosophers of technology, such as Ihde and, for instance, Verbeek,[26] have highlighted the enabling as well as constraining role of technologies and technological infrastructures (the script, the printing press, mass media, hyperlinked connectivity and computational in-betweens) in the co-constitution of self and lifeworld. Ihde and Verbeek speak of technology

[25] Merleau-Ponty (1945), Ricoeur (1976), Varela, Thompson, and Rosch (1991), Ihde (1990).
[26] Verbeek (2006).

in terms of mediation, emphasizing that such meditation entails different types of impacts on how self, mind and society are shaped. The introduction of the handwritten manuscript reconfigured our relationship to time and space; it enabled a distantiation between author and reader across geographically distant lands and between temporally distant eras. In a way, it liberated human beings from the tyranny of the here and now that prevails in face-to-face relations. Location was multiplied by imagined and remembered locations beyond the memory and forecasts of individual human minds. The externalization of memory has created both history and – paradoxically – a plethora of present futures that co-constitute the future present.[27] Computational mediations by what Greenfield has called the 'everyware',[28] reshuffle our connections to the locations we inhabit and those we visit, either 'in the flesh', electronically or virtually. As Julie Cohen has explained,[29] our sense of location multiplies: our embodied self sits behind a screen, while communicating via email, posting messages on SNSs, or while engaging in real time interactions in online gaming, video conferences and the more. Note that, currently, we have not the faintest idea of where the physical servers are *located* that allow us to send and receive messages, though we can no longer assume that they remain within the confines of a jurisdiction we know well enough to trust. Location matters, but its datafication uproots traditional properties of 'place' as a coordinate that is independent from 'time'.

How does our cybernetic point of departure relate to the Onli*f*e World? Thinking in terms of messages has the advantage of paying attention to the flow of information, while also taking into account that data can only mean something to *somebody* – data in itself is not just mindless but also meaningless. Viewing data as moving in a specific direction, from a sender to a receiver, enables to see data as content in the context of a specific relationship. Moving beyond the cybernetic focus on the *integrity* of the data that is 'transported' from one machine to another,[30] we can instead ask the question whether the same data means different things to the sender and to the receiver, and, if so, on what this depends. Is meaning agent dependent? If so, how can the agent-sender foresee how her message is understood by the agent-receiver? Can she tune her message in a way that increases the likelihood that the addressee gets the message that she is trying to convey? Might this depend on the role of the agent-addressee, and thereby on the context within which the message will be received? This connects with what was briefly discussed above, namely that a sender may intend to send a message to a

[27] Cf. Esposito (2011).
[28] Greenfield (2006)
[29] Cohen (2007).
[30] The integrity refers to the fact that the content of the message remains the same during the exchange. A similar focus is present in digital security: next to confidentiality and availability of data and systems, digital security is focused on making sure that the data sent is identical with the data received.

specific addressee, whereas the message is (also) received by one or more others.[31] As indicated, this introduces the notion of intent and raises the question of whether speaking of messages implies agency and what this means in the context of machine to machine messaging. These questions gain traction in an Onli*f*e World that is defined by the hidden complexity of vast layers of computational in-betweens and by the network effects of hyperconnectivity. How do agency, intent and the difference between addressee and receiver relate to informational location privacy in the Onli*f*e World? Does the emergence of an Onli*f*e environment afford something like 'the freedom from 'raw', networked and/or 'processed' location data being shared with others without consent or necessity'? Or should we acknowledge that the mindless agency of machine to machine communication renders both consent and necessity meaningless as effective constraints on the sharing of information? In the following sections I will investigate how informational location privacy defined in terms of the sending of messages, relates to the ethical concept of contextual integrity and the legal concept of purpose binding.

## 5. The ethical concept of contextual integrity

Informational location privacy implies that location matters to individual persons and relates to a sphere that requires boundary work.[32] The right to privacy is often defined in relation to the sanctity of the home as a physical location that shields the person from outside interference. To put it bluntly, this is the sphere where one can burb and scratch, get up late or sit through the night, eat, dance, read, drink and watch television without being supervised. Whereas we may wish to portray a certain image of ourselves when going off to work, visiting one's parents-in-law or when we walk the streets of an unknown city, the home provides for a space of retreat, of freedom from external constraints, from the gaze of the other and the from the investigative powers of both one's neighbours, the family and the state. I hope that the reader will detect a certain irony here, since the state has found its way into our homes via e.g. the interception of telecommunication; family is often – a potentially oppressing - part of the home environment; and neighbours can violate our sense of privacy by means of e.g. loud music or gossip. Nevertheless, the matter of walls, doors and windows indicates a solid, visible and durable kind of boundary work that differs from much of the

[31] This is core to digital security: it relates to the confidentiality and is usually discussed in reference to Alice sending a message to Bob, while Eve is evesdropping on them to overhear confidential information. See Leeuw and Bergstra (2007), and – just for fun: Gordon (1984).
[32] On privacy as boundary work rather than control Altman (1975).

boundary work required in an Onli*f*e World, where the borders between work, home and leisure have to be built into email traffic, facebook friending strategies and online websurf and purchasing behaviour patterns.[33] Simple oppositions such as private and public seem to lose their meaning in a world that sets the defaults for seamless bordercrossing between a host of different social spheres, allowing but also forcing onli*f*ers to continuously navigate the furiously overlapping contexts of e.g. employment, business, consumption, religion, health, family, politics and education. Navigating these 'furiously overlapping contexts' must take into account that messages sent within one context will often – though unintended – arrive in another context, notably due to the fact that most of these messages concern observed data instead of – or next to – volunteered data. Framed in another way, much observed data is 'gleaned', even though no message was sent

This raises the issue of context. In her ground-breaking work on the ethics of data sharing, Helen Nissenbaum has called for a more nuanced, more thoughtfull but also more practical understanding of what is at stake with informational privacy. After publishing pivotal work on 'privacy in public' and 'contextual integrity' – besides numerous other work e.g. on trust and security, Nissenbaum has expounded on the idea of privacy in context, explaining how we might rethink the integrity of social life.[34] In this section I want to explore how a cybernetic understanding of the right to privacy can be transformed by the broader scope and enhanced by the more precise articulation made possible by the introduction of the concept of contextual integrity. This, however, does not mean that a cybernetic understanding of privacy in itself brings no added value or can be discarded as merely reductive. As mentioned above, I believe that it is crucial to develop and operationalize conceptions of informational privacy that are interoperable with their cybernetic articulation, precisely because our Onli*f*e World is saturated with computational systems built on cybernetic assumptions.

Nissenbaum defines contexts as structured social settings, with characteristics that have evolved over time.[35] They are subject to a host of causes and contingencies of purpose, place, culture, historical accident, and the more. In traditional sociological and philosophical terms one could say that a context is an institution, a social sphere, a practice, entailing roles and patterns of interaction. Some of the examples she gives are health care, employment, education, religion, family and the commercial market place. Different contexts may overlap

[33] The introduction of personal computing and smart phones has blurred the borders between home, work and leisure, while it has enabled detailed monitoring of web surf behaviours that renders transparent one's personal preferences. On top of that, smart energy metering systems allow to detect unexpectedly granular lifestyle patterns, potentially providing an x-ray of what goes on within the home.
[34] Nissenbaum (2010).
[35] Nissenbaum (2010), 130ff.

or conflict, one context may 'nest' in another. In fact, I will argue that one of the most forceful challenges for contextual integrity occurs when one context monopolizes a specific domain or even an entire society (e.g. the context of religion may dominate the private sphere or even the political sphere as in a theocracy), or that one context colonizes another (e.g. the commercial market place may colonize higher education). Importantly, Nissenbaum suggests that context is not a formally defined construct, it cannot be represented in a final, definitive way. This does not mean that nothing can be said about what counts as a particular context, but one should always take into account that contexts are constituted by people and norms that are co-constituted by the contexts they navigate. Context is – I would suggest – firmly grounded in the thin air of our double contingency;[36] contexts *make us up* while we *make them up*. That being said, for individual persons the norms that constitute and regulate particular contexts are mostly given, even if they may find ways to challenge, test or transform them.[37] It may be, however, that this experiential fact – that we are somehow thrown into an already existing socially structured world – is less obvious than before. It seems that, first, the blurring of borders between different contexts and, second, the fact that a person can easily navigate different contexts from one location, has a lasting effect on the stability of contexts. The point is that contexts have to tune their song to the constant interference of competitive contexts that impose themselves and vie for our attention. When arguing for contextual integrity we should therefor acknowledge, first, that context is becoming a moving target and, second, that we are confronting a power play between the contexts of – notably - the political and the economic spheres on the one hand and the spheres of healthcare, education, employment and religion on the other hand. Populism and market fundamentalism may overrule common sense understandings of what matters in a healthcare or employment context and this raises the question of what contextual integrity means in terms of data flows.

Nissenbaum has proposed that a discussion of the ethics of data sharing should focus on data *flows* instead of singular data, and take its clue from the informational norms that regulate such data flows in a particular context. Instead of advocating a one-size-fits-all approach of informational privacy, she reinvents the notion of the legitimate expectation of privacy by paying trained attention to what can be legitimately expected within the context(s) in which the data flows take place. More precisely, she suggests distinguishing between norms of appropriateness (what types of data can be shared) and norms of distribution (who gets what information) as two types of informational norms that determine the sharing of information within and between contexts. What makes her framework pivotal for the

[36] Vanderstraeten (2007). Hildebrandt (2013b).
[37] Norms and contexts are co-constitutive, Nissenbaum (2010): e.g. 141.

articulation of informational norms is that she acknowledges that technologies co-constitute existing contexts, and one of the salient points she makes is that new technologies may transform existing contexts and/or create new contexts. This complicates the use of context as a measure for the integrity of information flows, but this complication has the added value of paying homage to the complexity of the Onli*f*e World, instead of reducing the playing field without providing any insight in what is at play.

The crucial 'constituents' of a context where information is shared are defined as: actors (sender, receiver, referent; which may overlap); attributes (types of information; noting that appropriateness of information flows is not one-dimensional, nor binary);[38] and transmission principles (for instance confidentiality, reciprocity, desert, entitlement, compulsion, need; this entails a rejection of simply dichotomies such as those between access and control). This set of constituents enables developing a privacy impact assessment heuristic (PIA heuristic) that traces the transformation of informational norms due to the introduction of novel technologies, described as socio-technical practices. This heuristic consists of nine steps: (1) describe the new socio-technical practice in terms of information flows (2) identify the prevailing context, (3) identify sender, receiver and referent, (4) identify the principles of transmission, (5) locate applicable entrenched informational norms and identify significant points of departure, (6) make a prima facie assessment, (7) perform the first evaluation in terms of what harms, threats to autonomy, freedom, power structures, justice, fairness, equality, social hierarchy and democracy are expected or have emerged, (8) perform a second evaluation by asking how the system or practices directly impinge on the values, goals, ends of the particular context, (9) dare to formulate a judgment for or against the new socio-technical practice under investigation.[39]

If we refer back to the extended version of the cybernetic definition of informational location privacy, we can check whether the decision heuristics of contextual integrity provides for new insights or a more apt operationalization. The definition was:

> The freedom from networked and/or 'processed' location data of a referent being shared with others without the referent's consent or necessity.

I have inserted the referent that was implied, to make the definition more explicit. Let's be reminded that 'sharing' implies a sender, an addressee, a receiver and an intention. What

[38] Nissenbaum (2010): 144.

[39] I believe that in our technology driven world it is becoming increasingly difficult to stand up against technological innovation, cf. Morozov (2013). An unbridled and unsubstantiated technological optimism colonizes our Onli*f*e World. We should, however, dare to accept the responsibility of 'civilizing' the engineers and companies that are reconfiguring our lifeworld. This means that we dare to judge the impact of innovation, after careful scrutiny; it does not – of course – mean that we reject innovation per se.

would it mean to apply the decision heuristic on informational location privacy? I suspect that the relevance of the heuristic will become apparent when testing the negative condition of 'consent or necessity'. Under EU law, consent means 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed',[40] and must be given 'unambiguously' to qualify as a ground for personal data processing,[41] while in the case of sensitive data (revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life) the consent must be explicit to qualify as a valid legal ground.[42] Under EU law, necessity refers to five alternative legal grounds: contract, a legal obligation, the vital interests of the data subject, the public interest or the legitimate interests of the so-called data controller (the legal entity that determines the purpose of data processing).[43] The question is, whether the *validity* of the consent or of the various grounds of necessity depends on the context in which data is sent or received. For instance, the answer as to whether consent is an *appropriate* ground for the sharing of 'processed' and/or networked location data, depends on the context. In the context of employment, for instance, I could imagine that the power inequalities between employer and employee render consent inappropriate and therefor invalid. Similarly the business interests of a firm that survives on the sale of inferred location data may not be a proper ground in the context of healthcare or religion.

What makes the decision heuristic of interest here is that it starts with the question of what is new in terms of a socio-technical practice. Rather then trying to develop universal and general rules on the processing of location data, we are asked to first describe the information flows within a new socio-technical practice that implicates location data. If we take the example of Apps on smartphones as a new socio-technical practice, we can describe a series of (new) information flows.[44] These concern location data (temporarily) stored on the device that are sent from the device to app developers, app owners, app stores, Operating Systems and device manufacturer plus third parties such as providers of analytics and advertising networks.[45] It should be clear that we are dealing with observed data, because most users do not intend to send their location data to any of these parties, though they may have provided formal consent in order to get the service they want from the app. This also means that we are

[40] Art. 2(h) Data Protection Directive D 95/46/EC (DPD).
[41] Art. 7(a) DPD.
[42] Art. 8(a) DPD.
[43] Art. 7 DPD, sub b-f.
[44] 'Apps are software applications often designed for a specific task and targeted at a particular set of smart devices such as smartphones, tablet computers and internet connected televisions. They organise information in a way suitable for the specific characteristics of the device and they often closely interact with the hardware and operating system features present on the devices.', cf. Art. 29 Working Party Opinion 02/2013 on apps on smart devices, WP202, p. 3.
[45] Art. 29 Working Party Opinion 02/2013 on apps on smart devices, WP202, p. 2 and 9-13.

talking about messages that are sent from a device to another computing system, enabled by so-called Application Programming Interfaces (APIs) that 'offer access to the multitude of sensors which may be present on smart devices', e.g. 'a gyroscope, digital compass and accelerometer to provide speed and direction of movement; front and rear cameras to acquire video and photographs; and a microphone to record audio. (…) proximity sensors. Smart devices may also connect through a multitude of network interfaces including Wifi, Bluetooth, NFC or Ethernet. Finally, an accurate location can be determined through geolocation services.'[46] Clearly, the different types and the amount of data that is sent indicates that location data can easily be networked with other data (the unique identifiers of the device, content data from the address book, stored pictures, credit card and payment data, phone call logs, browsing history and the more) and further processed to enable, for instance, targeted advertising or simply the sale of such 'processed' location data to large data brokers (who may share them with online social networking sites).[47] The relevant information flows are not limited to those between device and app service provider, but will be followed by a number of secondary, tertiary and further flows that are increasingly invisible and unforeseeable (unless in the most abstract way).

We have now described the new practice in terms of information flows (the first step). The second step asks to identify the prevailing context. This means that the answer to the question of whether sharing location data is appropriate cannot be given as a general rule. It depends on the context. If we take the context of travel we can proceed to the next step, taking into account that whatever the heuristic offers will be restricted to the context of travel; to figure out what the heuristic does in another context one has to carefully go through all the steps for that particular context. The third step asks to identify sender receiver and referent. Though we have already discussed that the location data are sent to app developers, OS and device manufacturers, app stores and third parties, we must now pay closer attention to the issue of what agent is doing the sending. Must we pretend that the app user is sending all this networked and/or 'processed' location data, or should we say that the device, the OS, the API or the app itself is the mindless agent? This is an important and interesting question. As far as I am concerned the question is more compelling than the answer. In fact, as mentioned above, we might say that it is the receiver of the data that is 'having the data sent' to itself, thus qualifying as the sender. The app user may in fact be sending location data to her fellow travellers, to her family back home, to potential fellow travellers, or to hotels or other service providers of her choosing. In that case she is obviously the sender of the

[46] Art. 29 Working Party Opinion 02/2013 on apps on smart devices, WP202, p. 4. Geolocation services have been described in detail in Art. 29 Working Party Opinion 13/2011 on Geolocation service on smart mobile devices, WP185.
[47] Hill (2013).

volunteered location data. This is not so regarding the observed and inferred networked and/or 'processed' location data that is sent to the app developers, the OS or the device manufacturer, the app store or third parties that re-use the data. What is important is to use the third step to, first, investigate whether the messages contain volunteered, observed or inferred location data and what this means for the identification of sender, addressee, receiver and third parties, and, second, to investigate what location messages are sent and/or received by machines, and what location messages are sent and/or received by natural or legal persons. Finally, the point of the exercise is to seek out what new actors enter the context: which senders and/or receivers did not get to send or receive networked or 'processed' location data before the advent of apps on smart devices? It should be clear from the above that in the context of travel a whole series of new actors enters the scene; apart from the fact that people are enabled to send their location to actors they might have shared with even before the advent of smart apps, as we have noted, their networked and 'processed' location data is sent to receivers they may not even be aware of.

The fourth step asks to identify transmission principles. This concerns both the principles that informed the context of travel before the advent of smartphone apps and the emergence of new transmission principles. Instead of falling into the trap of discussing the messages in terms of access or control of location data, the heuristic invites us to check how these apps transform the legitimate expectations of travellers as to confidentiality, reciprocity, desert, entitlement, compulsion and need. Interesting questions arise as to confidentiality: can app users be sure that the location data they send are properly secured against interception? should they understand that their location data are networked and 'processed' by third parties and may be sold to the highest bidder? Reciprocity may come to refer to the fact that app providers make their profits by selling personal data, in return for free services to the referent of those data. This certainly introduces an entirely new kind of reciprocity that is not openly negotiated but entirely implied; there is no clear pricing mechanism that provides transparency as to how the provision of what personal data relates to the service that becomes available. One could of course claim that service providers that render free services 'deserve' to get access to personal data, but this introduces a strange moral connotation into an exchange that has first been commercialized. To what extent are app users entitled to know about what happens to their location data? To what extent are app providers entitled to store and 'process' location data? Which data protection and intellectual property rights conflict at the heart of these novel information flows? Is it still possible to share one's location with others without also providing them to unknown, abstract entities, or are travellers more or less forced to allow the new data flows as a side effect? Can they escape this compulsion by changing the settings of the app, their OS or their device? Is there a need for the

multiplication of information flows and it this necessity proportional to the advantages for individual users, also in the long run?

The sixth step involves a prima facie assessment, followed by an evaluation in terms of harms and threats to autonomy, freedom, power structures, justice, fairness and the more. I will not undertake these assessments separately, but will integrate them in the second evaluation that inquires how the sharing of location messages impinges on the values, goals and ends of the context of traveling. This is a tricky business. The context of traveling, obviously, consists of several very different contexts, notably that of business travel, vacation and, for instance, lawful and unlawful immigration (including political and/or economic refugees). The assessment will have to be undertaken in the different sub-contexts, taking into account the values, goals, fairness, power structures and democratic participation that is implied in the case of vacationers, business trips and migration. They may all come to use similar apps and they may all taste some of the less desirable consequences of sharing location data. Customer profiling may cost vacationers money, because companies are enabled to engage in profitable and invisible price discrimination; a business traveller may find that the security of her location data was not guaranteed, allowing competitors to buy networked information they can use against her; a refugee may find himself at the mercy of sophisticated passenger profiling that pre-empt his intention to ask for political asylum.

The point of this exercise is not to attempt a full analysis of the workings of the decision heuristic in the case of networked, 'processed' and 'raw' location data in the context of travel. For such an attempt the voice of those who might be affected would have to be integrated and experts in the relevant context should be involved to explain how the apps may disrupt legitimate expectations. Here, my point was to *show* how the heuristic helps to uncover a plethora of important transformations in our Onli*f*e World that cannot so easily be grasped by applying general rules to individual cases. I believe that this is the crucial distinction between Nissenbaum's contextual integrity as a decision heuristic and the legal framework of data protection within the EU. Whereas the first introduces the concept of context as a constitutive bridge between individual and society, allowing for a more precise exploration of the empirical transformations and their normative implications, the latter remains somehow trapped in the gap between the general rule and the individual case. However, it should also be clear that whereas the decision heuristic provides for numerous occasions for reflection on the ethical implications of data sharing in the Onli*f*e World, it has no teeth, it cannot provide for legal effect; it lacks the conditions that enable the law to provide legal certainty. In the next section I will discuss how the legal concept of purpose binding can help to further interpret informational location privacy, by unravelling the intricacies of the legal principle of purpose binding, as enacted within the EU data protection

framework. Before engaging with that, let me conclude by noting that the decision heuristic on contextual integrity has greatly enriched the cybernetic articulation of informational location privacy as 'the freedom from networked and/or 'processed' location data of a referent being shared with others without the referent's consent or necessity'. It has traced the roles and connections of the senders and recipients of 'raw', networked and 'processed' location data, inquired into the transmission principles that 'fit' with a particular context, allowing for a more focused reflection on the difference between sharing volunteered data on the one hand and observed or inferred data on the other. It has thus provided a framework that gives direction to the investigation into the value and the validity of both consent and necessity, depending on the context of application, though taking into account that context has become a moving target. To some extent, the decision heuristic opens a conceptual toolkit to follow the transformations of contexts and their novel interpenetrations. In that sense I believe that it does what the Onli*f*e Initiative aims for: to reengineer our conceptual tools to create greater awareness of the impact of socio-technical change.

## 6. The legal concept of purpose binding

Law, however, is made of different stuff. Though, on the one hand, its procedural justice forces courts to suspend their judgement until the relevant voices have been heard and the facts have been investigated, on the other hand, legal certainty requires a decision. Even when the jury is still out on the ethical standards that should rule individual and institutional actions, courts must give their judgement. As the German legal philosopher Gustav Radbruch noted, people do not necessarily agree on what is morally just and at some point we need a decision that has the force of law, about which standards will orient societal interaction.[48] The law is not only after justice, or merely after utility. It also consolidates legitimate mutual expectations between those who may never meet, though they may exchange economic value, share data and contribute in defining the public interest. This signifies one of law's most important dimensions: that of legal certainty, the hallmark of positive law in modern society.[49] It connects the law to the authority of the state, while, in a constitutional democracy, also reigning in its *powers*, which are thus transformed into *competences*: enabling and limiting governments' power to act. This perspective on the law hinges on the

[48] Radbruch (1950).
[49] Cf. Radbruch (1950), who spoke of the antinomies of the law: legal certainty, justice (as fairness) and the purposiveness or instrumentality of the law.

intricacies of the internal and external sovereignty of the modern state. The offspring of this dual sovereignty is the so-called *Rechtsstaat* or the Rule of Law, that provides protection of individual liberty and mitigates the monopolistic tendencies of the power of police (in its old meaning of undivided government powers, including administration, legislation and adjudication).[50] We should note, however, that – paradoxically - this protection is dependent on the sovereignty it protects against, and admit that the historical artefact of the Rule of Law cannot be taken for granted in the era of Big Data Space and the Onli*f*e World.

Nevertheless, I will now investigate the notion of purpose binding as a principle that originates in one of the foundational principles of the Rule of Law: the legality principle (not to be confused with its ugly brother, legalism).[51] Legality refers to the fact that governments that are 'under the Rule of Law' can only act on the basis of the law: their legislative, administrative and judicial and other actions must all be based on the law and remain within the limits of the law. Under the Rule of Law the state is both *constituted* by and *limited* by the law. As a consequence, its decisions must be performed for the specific purpose for which a particular competence has been enacted. An explicit and specified purpose thus defines the competence to act, but also – in one and the same Act - restricts governmental actions to those that can be understood to further the relevant goal.[52] The goal is thus both enabling and limiting, in one and the same stroke. The constitutive and the regulative functions of this purpose are two sides of the same coin. Note that legality is not the same as legalism. The latter gives absolute priority to the written code of the legislator, potentially stifling any kind of innovation by requesting adherence to the written Acts of Parliament. The former goes further, by requesting that the legislator itself is under the Rule of Law, requiring that the goals it specifies are legitimate goals – taking into account the written or unwritten constitution and international human rights law. This also implies that whenever the state pursues goals in a way that threatens to interfere with the fundamental rights of individual citizens, such interference must be in accordance with the law, necessary in a democratic society and proportional to the legitimate aim.[53]

---

[50] On the power of police see Dubber and Valverde (2006). With the rise of the modern state in Europe legislation became more important as an instrument to issue general dictates to the subjects of the sovereign. This has been called the rule *by* law. Before the rise of the Rule *of* Law, courts spoke law in the name of the sovereign (*rex lex loquens*); judges were entirely under the rule of man (the king, the Parliament). Only when the courts managed to gain a measure of independence they were capable of standing up against the sovereign, in the name of the sovereign. This is called the paradox of the Rule of Law: *iudex lex loquens*. See e.g. Schönfeld (2008).

[51] On the difference between legality and legalism see (Hildebrandt 2008) my review of Dubber and Valverde (2006).

[52] Cf. e.g. Habermas' *Diskurs-Maxime* which dictates that legitimate actions must be such that they can be reconstructed as being in the general interest (Habermas 1996).

[53] This is known as the triple test for the justification of interference with the human rights of privacy, freedom of religion and freedom of speech in the European Convention of Human Rights.

It is not clear to me how the principle of purpose binding travelled from constitutional and administrative law to data protection legislation, though it seems an important research question to figure this out. The most important consequence of its migration to data protection is that it becomes applicable to big players that are not (part of) a government. Just like states, legal subjects that process personal data of individual citizens are required to specify a legitimate goal and, just like states, they are accountable for acting within the bandwidth of the purpose they specified. I will now clarify what the principle of purpose binding means in the context of data protection; how it relates to the distinction between volunteered, observed and inferred data; and how it stands with contextual integrity. Finally I will see how both contextual privacy and purpose binding can be framed in terms of sending messages containing 'raw', networked and 'processed' location data.

To understand what the principle means in terms of data protection we must position it in relation to consent, that is often considered to be the foundation of data protection. Within the EU legislative framework, however, the processing of personal data is conditioned by two types of legal requirements:[54] first, there must be a *legal grou*nd and, second, the processing must be *fair and lawful*. With regard to the first, the data protection directive (DPD) stipulates that one of six legal grounds must apply: only the first concerns (a) freely given and informed *consent*, the other five concern *necessity* in relation to (b) a contract, (c) a legal obligation, (d) the vital interests of the data subject, (e) the public interest or (f) the legitimate interests of the data controller (if these interests are not overruled by the fundamental rights of the data subject).[55] What is important is that *whichever* ground is applicable, the processing of personal data must *always* comply with the conditions of lawful and fair processing, the second type of legal requirements for the processing of personal data. One of these conditions is purpose specification, and another is use limitation, restricting the use of data to what is compatible with the purpose as specified.[56] This means that one *cannot* consent purpose limitation away; a valid new legal ground does not imply that historical data can now be used for an incompatible purpose in relation to the one for which they were originally processed.[57] Purpose binding thus ties whoever processes personal data to the explicit legitimate purpose as it was specified upfront, when the data were first collected. It chains that entity to its own stated – and necessarily legitimate - purpose. It should be obvious

[54] Next to a number of other requirements, notably those concerning transparency (information obligations).

[55] Art. 7 D 95/46/EC.
[56] Others see to the integrity of the data, meaning its completeness and correctness. Art. 6 D 95/46/EC.
[57] See on this the Art. 29 Working Group 03/2013 on purpose limitation, WP 203.

that this creates a friction with the mantra of Big Data, that seems to require collecting as much data as possible to enable unforeseeable novel correlations that create added value.[58]

The principle of purpose binding is connected with the central role of the data controller, i.e. the legal entity that determines the purpose of the processing of personal data. The data controller is *not* necessarily the entity that actually processes the data; it is, however, responsible for whatever processing is performed under its authority. If we relate this to the idea of a message, we can say that if a user of a location based service (LBS) shares her location data with a restaurant, this user may be termed the data controller, while the LBS is the data processor.[59] This is especially relevant if friends can share the locations of their friends with other friends. However, to the extent that the LBS uses the location data for its own purposes, e.g. for behavioural advertising or any other business model, the LBS is the data controller and is obliged to specify its purposes explicitly, at the latest when it starts processing the data. And, the LBS is not allowed to re-use the data for an incompatible purpose, nor is any other data controller allowed to do this.

All this should clarify that consent is not the most important principle of data protection legislation. Most messages containing 'raw', networked or 'processed' location data are sent for a purpose that is based on necessity: for instance, because a book is bought online the location is sent to enable delivery; or, because employers are legally obligated to send data on travel compensation for their employees to the tax authority; or, because a person is missing in a snow storm and the location of her phone may save her life; or, because a contagious disease requires knowledge of the precise location of contagious people; or, because the business model of a LBS depends on selling 'processed' location data, while it has taken measures to mitigate or even avoid interference with the fundamental rights of its users (for instance by means of anonymisation or pseudonymisation). But besides the fact that most personal data is not shared on the basis of informed consent, *even when it is* it must be processed only for the explicitly specified and legitimate purpose. This implies that to uphold data protection, purpose binding (the combination of purpose specification and use limitation) is the foundational principle, not consent. This is not just the case within the EU jurisdiction. Purpose specification and use limitation are part of the 1980 OECD Fair Information Principles that inspire most data protection regimes on a global level. Perhaps the major

[58] E.g. Massiello and Whitten (2010) on the added value of function creep (though this is not a term they use to refer to re-using data for novel objectives).

[59] Since it is the LBS that has created and offers the service one can of course argue that it is – for this reason – the 'real' or even the sole data controller. See, however, the Opinion of the Advocate General of the European Court of Justice (EcJ), regarding the question of whether Google, as a search engine, is a data controller or a data processor with regard to the content it indexes and ranks. Cf. the Opinion of Advocate General Jääskinen in Case C-131/12 of 25 June 2013 Google Spain v Agencia Española de Protección de Datos (the judgement of the EcJ is expected in 2014).

exception is the US jurisdiction that makes the application of this principle dependent on sectorial legislation.

Does this mean that in the US the question of whether, how and to what extent purpose binding applies depends on the context? Or should we rather expect that even within the EU jurisdiction the content and the scope of the purpose binding principle is largely determined by the context that is at stake? Or, should we understand the purpose binding principle at the global level as a legal instrument to sustain contextual integrity, because it enables data controllers in different contexts to determine different types of purposes? Or should we, finally, determine the scope of the purpose binding principle in view of whether it concerns volunteered, observed or inferred data – independent of context or jurisdiction? As to the latter, one can imagine that in the case of observed data purpose binding is less obvious because the purpose is practically invisible for the data subject, who is hardly aware of all the tracing and tracking that is going on. That might require more stringent application of the principle, but strict application easily irritates data subjects who keep getting messages about whether they agree that their location data is being mined, e.g. to improve the functionality of their navigator.[60] Again, much inferred location data concerns mobility or other patterns at the aggregate level, which means that the legal obligation to comply with the purpose binding principle does not apply, because these patterns do not – by themselves - render an individual identifiable. They rather allow to distinguish, target and discriminate different types of persons, depending on their residence, travel habits, work place, especially when linked with income, spending capacity, religion, sex, education, health. Location data then, is just one data point that helps to infer future behaviours, e.g. earning capacity, health risks or even morbidity.

Instead of providing unilateral answers to the questions I just raised, I will share my intuition that the *legal* obligation to comply with purpose binding has a complex relationship with the *ethics* of contextual integrity. Legally speaking, in the US jurisdiction the applicability of the purpose binding principle depends on the fragmented legal framework of data protection, which seems to differ per context. But this may have little to do with Nissenbaum's decision heuristic. I am not so sure that this heuristic underlies the choices made about whether or not to implement the principle in a particular sector.[61] That being said, the content and the scope of the purpose binding principle will probably vary in different

[60] This seems to be the case with regard to the obligation to provide prior informed consent for the use of tracing and tracking mechanisms, as stipulated – since 2009 - in the ePrivacy Directive (D 2002/58/EC). On this, art. 29 Working Party, Opinion 02/2013, on providing guidance on obtaining consent for cookies, WP 208; idem, Opinion 04/212 on Cookie Consent Exemption, WP 194.
[61] Though Nissenbaum (2010: 153-6) provides an interesting and convincing example, regarding the regulation of PII in financial transactions.

contexts, also within the EU jurisdiction.[62] For instance, in the case of commercial transactions the scope of the purposes that can legitimately be determined by the data controllers (companies) is fundamentally different from the scope in the context of healthcare. The latter requires very precise and narrowly defined purposes to minimize potential harm to the mental and physical integrity of patients, even though we should acknowledge that the advent of Big Data Space incentivizes the collection of ever more health-related data and the Onli*f*e World invites people to share health data with their peers in settings similar to SNSs. This relates to the requirement of proportionality between the legitimate aim of data processing and the infringement of e.g. human dignity. The context of commercial transactions seems to allow very broad and vague purpose specifications that include selling personal data for a profit, even though many would object to these practices.

The real problem here seems to be that the context of eCommerce tends to colonize other contexts in the Onli*f*e World, requiring e.g. newspapers, energy saving services and basically any other utility or public interest – including healthcare - to reinvent their 'business case' in terms of the sale of personal data. Purpose binding may blend into this by allowing organisations to reframe their purposes in terms of the added value created by collecting Big Data. To the extent that this happens, purpose binding cannot sustain contextual integrity, precisely because various contexts are overruled by the context of commercial gain.[63]

It is crucial to keep in mind that purpose binding, at least in the EU jurisdiction, is a legal obligation. It is articulated as a side constraint on the processing of personal data. The decision heuristic on contextual integrity, however, is not a legal obligation, but an attempt to frame an ethics of data sharing; it raises a number of empirical as well as normative questions that increase the reflective underpinnings of whatever the outcome is. This enhances the robustness of the outcome. One of the connections between contextual integrity decision heuristic and purpose binding could therefor be that the rigorous reflection of the first should feed into the interpretation of the second. This should help to prevent a reduction of legality to legalism; when law is separated from ethics it ceases to qualify as law,[64] it becomes

[62] In deciding whether further processing (re-use) of personal data is still in line with purpose binding requirement, the DPD demands that the purpose of further processing is not incompatible with the explicitly specified purpose for which the data was collected. The decision on whether a new purpose is compatible depends, amongst others, on the context. See, in more detail, Art. 29 Working Party, Opinion 03/2013 on purpose limitation, WP 203.

[63] The introduction of the notion of pseudonymous data in the draft General Data Protection Regulation as adopted by the LIBE committee of the European Parliament is highly problematic for this very reason: it assumes that if data controllers have a legitimate interest in the processing of personal data, this processing will be assumed not violate the fundamental rights of the data subjects if the data has been pseudonymised.

[64] This does not imply that law is equivalent with ethics. See Radbruch (2006) on the importance of legal certainty as the distinctive characteristic of law, compared to justice; at the same time, however, Radbruch warns that law that does not strive for justice no longer qualifies as law.

administration. Therefor, I believe that the EU Data Protection Impact Assessment – another legal obligation – could benefit from decision heuristics such as the one developed by Nissenbaum. This should help to inform the *quality* of the purpose specification and the *mindfull compliance* with the subsequent use limitation. Thus, purpose binding also feeds back into the contextual integrity decision heuristic, by means of a careful investigation of what new purposes are enabled by new technologically mediated information flows. Even more to the point, we should investigate how Big Data Space relates to the idea that data controllers can only process personal data for 'old' purposes. As we all know, anonymisation and even pseudonymisation do not resolve this problem, because precisely in Big Data Space increasingly enables deanonymisation.

This brings me back to the definition of informational location privacy and the question of its definition in terms of a message. To integrate both the principle of purpose binding and the concept of contextual integrity we can extend the definition:

> Informational location privacy is *the freedom from* 'raw', networked and/or 'processed' location data of the referent, the sender, the addressee or the receiver of a message being shared with others without consent or necessity, and *the freedom from* such location data being shared for purposes incompatible with the explicitly specified and legitimate purpose for which it was first collected.

Please note that this definition is not equivalent with the EU or US legal rights to data protection for location data. It is a definition in terms of the sending of messages, containing 'raw', networked and/or 'processed' location data, not merely about the processing of data. It is about data flows, rather than data processing. It is about 'raw', networked and/or 'processed' location data being send between machines, between humans or between humans and machines; not about intra-machine processing of data. This has advantages and drawbacks, as indicated above. The definition applies to volunteered, observed and inferred location data, but only insofar as they are 'of' the referent, the sender, the addressee or the receiver of the data flows. Insofar as inferred data are patterns, profiles or correlations at an aggregate level, they are outside the scope of the definition, but as soon as they are applied to the referent, sender, addressee or receiver they are part of the definition (under 'processed' location data). The added advantage of this definition, next to the shift from individual data to flows of information, is that it highlights the agency – and patiency - of those involved (sender, addressee, receiver, referent).[65] Instead of treating the agents (sender, receiver) and the patients (referent, addressee) as separate entities, they are viewed here in the context of

[65] On the salience of thinking in terms of both agency and patiency see e.g. Floridi and Sanders (2004). The agent is whoever acts morally relevant, the patients is whoever is affected in a morally relevant way. The concept of patiency goes back to Aristotle's *Physics*.

the relationship they have when sending and receiving messages, and/or when being the addressee or the referent of such messages. The framing of informational location privacy in terms of messages can thus clarify the reciprocity of the relationships, the power structures they involve, the responsibility (liability) for the actions undertaken and the importance of rights for those affected by these messages.

Should we integrate the contextual privacy heuristic into the definition? One answer could be that the heuristic sees to an investigation that should occur before novel technologies are introduced, or while designing legislation to enable and constrain their employment. As developed, the heuristic is not focused on the question of *what is* informational privacy but on *how technologies impact contextual privacy and whether this is acceptable*. As argued above, I think that the notion of contextual privacy can, nevertheless feed into the interpretation of the principle of purpose binding, notably by the courts, by demanding focused attention to what the context of application requires. This would extend the definition as follows:

> Informational location privacy is *the freedom from* 'raw', networked and/or 'processed' location data of the referent, the sender, the addressee or the receiver of a message being shared with others without consent or necessity, and *the freedom from* such location data being shared for purposes incompatible with the explicitly specified and legitimate purpose for which it was first collected, taking note of what the context *within which* or the contexts *between which* messages are or may be shared requires.

This is too long a definition for everyday usage. It captures what is at stake, but is on the verge of turning into 'legalese'. Nevertheless, I believe that the exercise of developing this definition helps to enrich our understanding of what informational location privacy means. As the reader may know, my own favourite working definition of the right to privacy is 'the freedom from unreasonable constraints on the building of one's identity'.[66] Where the former definition is very detailed, the latter is very abstract. The point is that the sharing of 'raw', networked and/or 'processed' location data in the era of Big Data Space, in an Onli*f*e World, can constrain the building of one's personal identity in numerous ways. We must insist that these constraints are reasonable and one way of determining the reasonableness is to require consent or necessity *as well as purpose binding*, and to investigate how novel constraints fit with the contexts of application.

I conclude with the observation that the biggest challenge to *contextual integrity as a precondition for informational location privacy* may be that the context of commercial benefit and monetary added value seems to colonize all other contexts. If we do not figure out how to

[66] Cf. e.g. Hildebrandt (2008).

preserve the capability of individual citizens to develop legitimate expectations for the sharing of 'raw', networked and 'processed' location data within and between different contexts, the idea of informational privacy may become an empty shell. The threat is not that the institution of context is a moving target, though this presents a formidable challenge. The more complex threat may be situated in the surreptitious colonization of any relevant context by the dictates of commercial enterprise. This 'colonization' can easily turn the PIA decision heuristic as well as the purpose binding principle into lame ducks, e.g. by translating contextual appropriateness or the scope of a compatible purpose into the outcome of a balancing act between anything and economic value – thus nicely complying with the side constraint that stipulates the requirement to perform such a balancing act.

## 7. Conclusions: Framing the Balancing Act For Location Messages

One of the objectives of this chapter was an investigation into whether, and if so, under what conditions and how contextual integrity and purpose binding form either side constraints on the free flow of information, or require a balancing act between the civil liberties of individual citizens and the free flow of information. Instead of proceeding straightforwardly to answer this question, I have taken a more oblique way of tackling the issue. It is clear, upfront, that the PIA heuristic and the purpose binding principle are formulated as side constraints: they both require that specific steps are taken and conditions fulfilled before the sharing of 'raw', networked and 'processed' data is either ethically right or lawful. When taking a more in-depth view of both, we encounter various requirements that actually consist of a balancing act, e.g. the last step in the decision heuristic (weighing the impact of novel technologies on the transmission principles regarding 'raw', networked and 'processed' data to decide their acceptibility), and the proportionality test that determines the legitimacy of the personal data processing in relation to the purpose (notably the five legal grounds that involve necessity).

This – prima facie – answer does not bring much news. To generate potentially new perspectives I have formulated the concept of informational location privacy in line with the cybernetic approach to communication, defining it as the freedom from specific types of messages. I have argued that this has three advantages. First, it translates the problem into the language of information theory that is at the root of the development of the computational systems that increasingly determine our lifeworld. This has spurred investigations into Big

Data space and the Onli*f*e World. Second, it focuses on information flows instead of discrete data, which is pivotal in the era of Big Data Space and the hyperconnectivity that is prevalent in the Onli*f*e World. Third, it highlights the agency and the patiency of both humans and machines as senders, addressees, receivers and referents of location messages, instead of disentangling these agents/patients from the messages and information flows in which they are implicated. This is again pivotal, in the era of the Onli*f*e World where the heteronomy of human-machine relations transforms both self and society. Taking into account that there are three types of location data: volunteered, observed and inferred, I have extended the cybernetic definition of privacy with an explicit indication of the type of location data at stake. That is, I have distinguished between volunteered and observed location data in itself ('raw' data), volunteered and observed location data that is linked with other data (networked data) and the inferred data resulting from data mining operations on 'raw' and networked location data ('processed' data, which also includes location data inferred from other types of data). I have added the notion of intent, that is implied by the concept of 'sending'. To keep machine-to-machine communication in the loop I view intent at the highest level of abstraction, that includes the mindless intent of machines. Intent implies that next to the sender, the receiver and the referent, the addressee (the intended receiver) becomes part of the definition (which may overlap with the receiver but this need not be the case). Intent also implies that sending a message has a purpose. The fact that a message has a purpose does not necessarily mean that this purpose is achieved, nor does it imply that the receiver has the same purpose as the sender. Precisely by differentiating the actors and patients it becomes possible to stress the role that purposes have in the sending of messages, raising questions about who determines that purpose, who is accountable for its determination and/or compliance and the question of whether and under what conditions the referent of a message can veto messaging if she does not agree with its purpose. The DPD defines all these positions, but it helps to take some distance from the monolithic assumptions that underlie the different roles in the DPD, e.g. by noting that people can be data subjects and data controller with regard to the same location message, depending on who is the addressee (e.g. one's friends) and who is the receiver (e.g. the service provider).[67]

Speaking of location messages is less anonymous than speaking of location information flows, while, like the terminology of location information flows, it spotlights that a location message may be sent from one context but be received in another (whether on purpose, by accident or due to eavesdropping). Thinking in terms of senders, receivers, addressees and referents also helps to understand the importance of the distinction between volunteered, observed and inferred data. Observed data were not sent to the receiver, unless

[67] The DPD does not exclude this possibility, but the implications are as yet unclear.

we equate the receiver with the sender (establishing that a data controller that observes behavioural data actually sends that data from the device of the referent to its own servers). Inferred data can be produced by means of intra-machine computations, which does not involve a message, but techniques such as machine learning may infer data by learning from the 'messages' they pick-up from their environment.[68] The most salient form of inter-machine messaging that produces inferred data is that of multi-agent systems, whose emergent behaviour informs so-called simulation games.[69] Such simulations are increasingly employed to design the various layers of automated decision systems, e.g. in the case of the smart grid. The assumptions built into such systems have potentially ground-breaking implications for contextual integrity as they may enable the sending of e.g. 'raw', networked or 'processed' location data outside the context where the initial messages were exchanged. One example is the employment of energy usage data associated with a particular location to detect social security fraud. Another is the use of flexible pricing to incentivize new business models for value added services, which may invite business models that correlate the location of the 'energy user' with lifestyle and purchasing habits.[70]

Purpose limitation thus has its limits. If, at the moment that location data are first observed, volunteered or inferred, a multiplicity of purposes is already specified (e.g. to provide electricity, to send the bill, to detect social security fraud, to send targeted advertising, to enhance customer relationship management with value added services), the protection against a violation of contextual integrity might be nihil. It is, then, a side constraint that can easily be complied with, without providing substantial protection. From a legalistic perspective this may not be a problem, but such an interpretation of purpose binding flies in the face of the legality principle. Legality means that people have the capability to develop legitimate expectations and this capability is not a character trait but something a society affords by organizing things in one way rather than another.[71] The lack of legitimacy generated by the multiplicity of purposes may be remedied by integrating the decision heuristic of contextual integrity into the decision process on what purposes and what legal

[68] This raises the question of whether the feedback that a machine 'receives' has been sent by its environment or is merely 'perceived'. I would suggest that this depends on the measure of agency of whichever part of the environment is either sending or being perceived. On agency at the high level of abstraction of autonomous machines Floridi and Sanders (2004); on human agency as a special type of agency Hildebrandt (2011).

[69] These games may build on traditional assumptions of economic theory, as integrated in game theory, or, alternatively, they may incorporate the insights of behavioural economics and cognitive psychology. Both build on methodological individualism and adhere to the ideal of a rational decision making process. The main difference is that behavioural economics concludes that humans are biased and need help to become rational. The supposed biases described in cognitive psychology are often used to influence – if not manipulate – people's behaviour, notably in the realm of policy science and marketing. Cf. Thaler and Sunstein (2008).

[70] On the implications of profiling in the context of the Smart Grid within the EU jurisdiction Hildebrandt (2013c).

[71] Cf. Robeyns (2005).

grounds are legitimate. Which transmission principles are bent, transformed or eroded to accommodate the plethora of novel purposes that mushroom in the Onli*f*e World? What fairness is tweaked, which reciprocity is broken, does a new purpose unbalance existing power relationships? Or does it increase already existing power asymmetries that cannot be justified? Thus, the substantive protection that purpose limitation aims to provide under the heading of legality may be re-enabled by paying keen attention to the legitimate expectations within and between particular contexts. This solution, however, depends on boundary work between, on the one hand, the contexts of politics, health, employment and others, and that of economic markets on the other hand. In an era where the context of economic markets tends to overrule any other context, we may need to rethink the relationship between partially overlapping spheres of life, otherwise the outcome of any balancing act becomes polluted by the monolithic dictates of one particular logic.

**References:**


Amoore, Louise. 2011. "Data Derivatives On the Emergence of a Security Risk Calculus for Our Times". *Theory, Culture & Society* 28 (6) (november 1): 24–43.

Altman, Irwin. 1975. *The Environment and Social Behavior. Privacy Personal Space Territory Crowding*. Montery: Brooks/Cole.

Beresford, Alastair R., and Frank Stajano. 2003. "Location Privacy in Pervasive Computing." *Pervasive Computing* (January-March): 46–55.

boyd, danah, and Kate Crawford. 2011. "Six Provocations for Big Data". SSRN Scholarly Paper ID 1926431. Rochester, NY: Social Science Research Network. http://papers.ssrn.com/abstract=1926431.

Cohen, Julie E. 2007. "Cyberspace As/and Space." *Columbia Law Review* 107: 210.

De Hert, P., and S. Gutwirth. 2006. "Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power." In *Privacy and the Criminal Law*, edited by Erik Claes, Antony Duff, and S. Gutwirth. Antwerpen Oxford: Intersentia.

Dubber, Markus Dirk, and Mariana Valverde. 2006. *The New Police Science. The Police Science in Domestic and International Governance*. Stanford: Stanford University Press.

Esposito, Elena. 2011. *The Future of Futures: The Time of Money in Financing and Society*. Edward Elgar Pub.

Floridi, Luciano, and J.W. Sanders. 2004. "On the Morality of Artificial Agents." *Minds and Machines* 14 (3): 349–379.

Galison, Peter. 1990. "Aufbau/Bauhaus: Logical Positivism and Architectural Modernism." *Critical Inquiry* 16 (4): 709–752.

Gitelman, Lisa, ed. 2013. *"Raw Data" Is an Oxymoron*. Cambridge MA - London, England: MIT Press.

Gordon, John. 1984. "The Alice and Bob After Dinner Speech." http://downlode.org/Etext/alicebob.html.

Greenfield, Adam. 2006. *Everyware. The Dawning Age of Ubiquitous Computing*. Berkeley: New Riders.

Habermas, Jürgen. 1996. *Between Facts and Norms : Contributions to a Discourse Theory of Law and Democracy*. Studies in Contemporary German Social Thought. Cambridge, Mass.: MIT Press.

Hayles, N. Katherine. 1999. *How We Became Posthuman. Virtual Bodies in Cybernetics, Literature, and Informatics*. Chicago: University of Chicago Press.

Hildebrandt, M. 2008. "Profiling and the Identity of the European Citizen." In *Profiling the European Citizen. Cross-Discplinary Perspectives*, edited by M. Hildebrandt and S Gutwirth. Dordrecht: Springer.

———. 2008. "Governance, Governmentality, Police and Justice: A New Science of Police." *Buffalo Law Review* 557-598 (2): 557.

———. 2011. "Criminal Liability and 'Smart' Environments." In *Philosophical Foundations of Criminal Law*, edited by Antony Duff and Stuart Green, 507–532. Oxford: Oxford University Press.

———. 2013a. "Slaves to Big Data. Or Are We?"

———. 2013b. "Profile Transparency by Design: Re-Enabling Double Contingency." In *Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology (Hardback) - Routledge*, edited by M Hildebrandt and E. De Vries. Abingdon: Routledge.

———. 2013c "Legal Protection by Design in the Smart Grid". Report commissioned by the Smart Energy Collective (SEC). Nijmegen: Radboud University Nijmegen.

Hill, Kashmir. 2013. "Facebook Joins Forces With Data Brokers To Gather More Intel About Users For Ads." *Forbes*. February 27. http://www.forbes.com/sites/kashmirhill/2013/02/27/facebook-joins-forces-with-data-brokers-to-gather-more-intel-about-users-for-ads/.

Husserl, Edmund. 1970. *The Crisis of European Sciences and Transcendental Phenomenology; an Introduction to Phenomenological Philosophy*. Evanston: Northwestern University Press.

Ihde, Don. 1990. *Technology and the Lifeworld : From Garden to Earth*. The Indiana Series in the Philosophy of Technology. Bloomington: Indiana University Press.

———. 2008. *Ironic Technics*. Automatic Press.

Leeuw, Karl Maria Michael de, and Jan Bergstra, ed. 2007. *The History of Information Security: A Comprehensive Handbook*. 1st ed. Elsevier Science.

Massiello, Betsy, and Alma Whitten. 2010. "Engineering Privacy in a Age of Information Abundance." In *Intelligent Information Privacy Management*, 119–124. AAAI.

Mayer-Schönberger, Viktor, and Kenneth Cukier. 2013. *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Boston: Houghton Mifflin Harcourt.

Merleau-Ponty, M. 1945. *Phénoménologie de La Perception*. Paris: Gallimard.

Morozov, E., and Evgeny Morozov. 2013. *To Save Everything, Click Here: The Folly of Technological Solutionism*. New York: Public Affairs.

Nissenbaum, H.F. 2010. *Privacy in Context : Technology, Policy, and the Integrity of Social Life*. Stanford, Calif.: Stanford Law Books.

Prins, Corien. 2006. "When Personal Data, Behavior and Virtual Identities Become a Commodity: Would a Property Rights Approach Matter?" *SCRIPT-Ed* 3 (4): 270–303.

Purtova, Nadezhda. 2012. *Property Rights in Personal Data: A European Perspective*. Alphen aan den Rijn, The Netherlands: Kluwer Law International.

Radbruch, Gustav. 1950. *Rechtsphilosophie. Herausgegeven von Erik Wolf*. Stuttgart: Koehler.

———. 2006. "Five Minutes of Legal Philosophy (1945)." *Oxford Journal of Legal Studies* 26 (1): 13 –15. Available at: http://ojls.oxfordjournals.org/content/26/1/13.short.

Ricoeur, Paul. 1976. *Interpretation Theory*. Texas: Texas University Press.

Robeyns, Ingrid. 2005. "The Capability Approach: A Theoretical Survey." *Journal of Human Development* 6 (1): 93–114.

Schönfeld, K.M. 2008. "Rex, Lex et Judex: Montesquieu and La Bouche de La Loi Revisted." *European Constitutional Law Review* 4: 274–301.

Thaler, Richard H., and Cass R. Sunstein. 2008. *Nudge : Improving Decisions about Health, Wealth, and Happiness*. New Haven: Yale University Press.

Vanderstraeten, Raf. 2007. "Parsons, Luhmann and the Theorem of Double Contingency." *Journal of Classical Sociology* 2 (1): 77–92.

Varela, F.J., Evan Thompson, and Eleanor Rosch. 1991. *The Embodied Mind. Cognitive Science and Human Experience*. Cambridge, Massachusetts: MIT.

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

Wiener, Norbert. 1948. *Cybernetics: Or Control and Communication in the Animal and the Machine*. Cambridge MA: MIT Press.

World Economic Forum. 2011. "Personal Data: The Emergence of a New Asset Class." Available at http://www.weforum.org/issues/rethinking-personal-data.

World Economic Forum. 2012. "Rethinking Personal Data: Strengthening Trust". Available at http://www.weforum.org/issues/rethinking-personal-data.