Value-based Engineering for Ethics by Design

S. Spiekermann *Member, IEEE* and T. Winkler *Member, IEEE*

Abstract—This article gives an overview of value-based engineering for ethics by design. It is a foundational article that integrates the most important challenges and measures involved in eliciting, conceptualizing, prioritizing and then respecting values in system design. The methodology presented in this article does not only draw from software engineering, value sensitive design, design thinking, participatory, and co-design, but also from the philosophy of Material Value Ethics that gives this new field of ethical engineering a philosophical foundation. It is rounded up by a discussion of the timely challenges for value-based computing, including compatibility with popular agile forms of system development, the problem of responsibility in hardly controllable eco-systems of interconnected services, the fearless integration of diverse external stakeholders in value elicitation and prioritization and the difficulty in measuring the ethicality of a system. Finally, the value-based engineering methodology presented here benefits from learnings collected in the IEEE P7000 standardization process as well as a case study that was conducted by the authors of this paper in support of this effort. P7000 has been set up by IEEE to establish a process model, which addresses ethical considerations throughout the various stages of system initiation, analysis and design.

Index Terms—value sensitive design, values, ethics, ethics by design, system engineering, software engineering, design, risk management, privacy, security

A. Introduction

The past ten years have confronted the engineering world with shocks related to the ethics of technology design. The Snowden revelations, massive increase of cyberattacks on corporate and public infrastructures, an explosion of identity theft incidents and the rise of surveillance capitalism show how vitally important privacy and security have become as values to be considered during system design. The Boing 737 Max crashes made clear how the values of system safety, transparency and pilot control can fatally interact with the business values of profit and speed. The Cambridge Analytica case showed how social networks can undermine the value of democracy by allowing for privacy-intrusive manipulation and disinformation of users. Moreover, gurus of today's tech-world like Elon Musk or Bill Gates warn of major threats accompanying the spread of AI systems. Against this background, the engineering world finds itself confronted with the demand and challenge to build systems that acknowledge, incorporate and respect human values. More than ever, engineers today are held responsible for societal effects of the artefacts they built. Societal impacts can turn out as boomerangs of critique and legal trials if potential negative effects are not anticipated and cared for in the design of a technical product.

But how can engineers and the companies they work for meet this ethical challenge? How can they build systems in a way that systematically anticipates negative value potentials and works towards curbing them? And could values - which by their linguistic root stand for "something worthwhile"- not be considered as a positive mission in system design rather than a compliance exercise to defend against the worst?

So far there is no systematic engineering approach available that allows companies and their engineering teams to realize what experts call "*Ethics by Design*" [73]. Several established research communities are working towards Ethics by Design. These include scholars working on values in computing [1, 2, 3], in particular Value Sensitive Design (VSD) [2], Machine Ethics [4, 72], and Participatory Design [5, 60]. Some companies engage in privacy, security and safety assessments such that they lead into a privacy, security or safety *by design* [6, 7]. However, a general embracing of human value requirements has not yet happened in engineering.

One reason for this lack of adoption might be that the academic and practical efforts around values in computing are scattered. There is no consistent, usable method that companies could follow step-by-step and across-industries and that allows to both identify value principles and translate them into the engineering practice (x). Even if companies were willing to embrace any of the 84 value principles lists on ethical AI that have been published in the past few years [8], they would probably not know how to. None of these value lists calling for privacy, transparency, fairness, accountability, dignity etc. offer systematic guidance on how to go from such ethical value principles to practice. Mostly, they do not even contain proper definitions of the principles they call for [8]; for instance what privacy or dignity actually is. There is no common terminology established yet in the engineering world to consistently discuss

- *Sarah Spiekermann-Hoff chairs the Institute for IS & Society at Vienna University of Economics and Business, Welthandelsplatz 1, 1020 Vienna, E-mail: sspieker@wu.ac.at*
- *Till Winkler is a Ph.D. student at the Institute for IS & Society at Vienna University of Economics and Business, Welthandelsplatz 1, 1020 Vienna, E-mail: winkler@wu.ac.at*

Ethically aligned Design or what has alternatively been coined "Ethics by Design". In short, there is a deep need for a systematic value-based engineering method and a shared terminology. This article addresses this need. In order to do so, we embrace the timely literature on values in system design, combine it with a century of philosophical insight in Material Value Ethics, and benefit from expert knowledge that has been gained from a four-year long IEEE standardization process. This standardization work, which was conducted under the acronym "P7000" was set up in 2016 to establish a process model for addressing ethical considerations throughout system initiation, analysis and design.[1] The lead author of this article has been the permanent co-chair of this standardization, main author of the initial draft as well as a co-imitator of its set-up. Both authors have had editing roles throughout the years. Whenever there is reference being made hereafter as to "expert views", then these are stemming from the standardization work. Furthermore, our arguments here are supported by a real-world case study with a Telemedicine start-up (called "TM" hereafter). The authors of this paper conducted this academic case study with a real-world partner in order to support of the IEEE P7000 effort. TM is a medical platform planning to offer a video-chat-based diagnosis service. Its unique selling proposition is supposed to be a database that allows patients to be forwarded by TM doctors to medical specialists who have been ranked highly by colleagues. The case is described in the last section of this paper as well as in more detail in [65].

When using the term "engineer(s)" hereafter it is important to note that we do not only refer to system and software developers. Instead we recognize that a system coming-into-being is often co-determined today by project teams that include computer scientists, electrical engineers, product managers, legal scholars and many more. In close co-operation these individuals "engineer" a system that they want to bring to market. So, engineers are broadly defined here as those members of an innovation team who influence the values, goals, architecture, data flows, policies, hardware and software components of a system. In organizations that follow an agile or design-thinking approach to system development the engineering team can even include users who give feedback on prototypes or finished artefacts on a regular basis [21, 22]. We are aware that with this definition of "engineering" we go beyond the classical understanding of the term and we embrace a vision for engineering that others have also referred to as "co-design" [3, 68].

The article is structured as follows: First we argue why ethically aligned design should be built on values. We describe what values are from a philosophical perspective and how terms can be made useful for engineering. After this introduction to the value space we dedicate the rest of the article to the description of the value-based engineering methodology alongside to phases: Ethical Exploration and Ethically aligned Design, well aware that these two phases constantly iterate in practice. We describe vital preparation steps for value-based engineering, core processes, and a case study illustrating the value exploration phase specifically. Throughout the article we subsequently develop definitions for all relevant value engineering constructs and accumulate 12 methodological requirements and 17 related recommendations that capture the key ingredients of value-based engineering in a nutshell.

B. Three Foundational Questions for Value-Based Engineering

Pioneering groundwork for value-based engineering has been done in the past twenty years by the VSD community [2, 12], complemented by other scholars who have used the concept of values for system design [e.g. 1, 27, 66, 12, 34]. Through many conceptual and applied research efforts, the concept of values has become the core of today's ethical computing efforts and stands at the center of political calls for ethics in AI [8]. But using values for ethical engineering is not a given. Competitive concepts such as human rights and norms have been positioned as alternative approaches and no effort has been done so far to ensure that the engineering domain benefits from the learnings of an entire century of value philosophy. So why should Ethically aligned Design be founded on values? What are they? And how is the ethicality of a system linkable to values at all?Why should Ethically aligned Design be founded on values?

The reason for centering Ethically aligned Design specifically on values, instead of norms, needs or human rights, is manifold: The value concept is grounded in a rigorous body of philosophical knowledge first established by scholars like Max Scheler [11] and Nikolai Hartmann [13]; today driven by philosophers like Eugene Kelly [10]. This work conducted under the term "Material Value Ethics" is complemented by the rediscovery of the closely related Aristotelian virtue ethics; specifically in the 2nd half of the 20th century both in philosophy and management [61, 62, 63]. Virtues, such as courage, generosity or politeness are values carried by persons. They are particularly relevant for technology design [14]. Against this background it is not surprising that established university textbooks on Computer Ethics have been focusing on values for quite some time [4, 27].

Embracing values seems wiser for technology design than focusing on human rights, social norms or needs. All *human rights* are values themselves, for instance dignity or liberty. They are corresponding to what is valuable in humans' lives [13, p.64 ff.]. But there are more values than established rights. Just think of values relevant in system design such as beauty, perfection, control, transparency, etc. for which there are no established human rights. Values open engineering efforts up to the widest possible spectrum of positive and negative potentials whereas human rights can only represent those human values that are recognized already as rights in international treaties.

Besides a call for respect of human rights, some computer ethics scholars have argued for *norms* to be the driving force of ethical system design [15]. Norms are culture-specific representations of acceptable group conduct. However, norms have historically failed to protect humans from harm. A drastic example to illustrate this failure is Nazi Germany, which built up inhumane norms and tuned its technology accordingly. For example, Nazis imposed the (negative) norms of anti-judaism and arianism on many Germans who did not share in this norm. Norms therefore always need to be challenged first as to their goodness; that is the positive value they effectively bring to a society. Positive values are the pre-condition for working with corresponding norms in system design. That said, building norms of behavior *as value dispositions* into a system, such as the norm of formal address, distance keeping, etc can help a value such as dignity or politeness to unfold (15). So effectively, values can be a starting point for deriving relevant norms of system behavior.

Some scholars have promoted a focus on *needs* when designing systems [67]. A need typically results from the shortage of something valuable. Especially the "design thinking school" has been using needs as the conceptual basis for innovation, going far beyond functionality-driven forms of innovation.[2] However, many ethical issues of today's systems, such as privacy, control or transparency, are often not perceived as a shortage by end-users. Again, values are the broader concept: They include needs, because needed is only what is valued. That said, stakeholder needs can help to prioritize systems' value potentials, because values for which there is a necessity or a shortage might deserve special attention. Values however also allow to embrace the good, true and beautiful in their own right and thus go beyond what might be needed. Value-based engineering is about the bigger mission.

1) What are values? And what terminology is useful to value-based engineering?

As the first two pages of this article show it is possible to write about values without defining them. We all have an intuitive conception of them, *"a conception … of the desirable which influences the selection from available modes, means and ends of action"* (p. 395 in [9]). They are *"principles of the ought-to-be"* writes Nikolai Hartmann (p. 98 in [13]). That is however only when they are positive, because as Scheler has shown, values can also be negative. What ought to be in principles is equally defined by what should not be. Therefore, Material Value Ethics postulates the following value axioms which can be directly applied to value-based engineering (p. 206 in [11]):

1) The existence of a positive value is itself a positive value.
2) The non-existence of a positive value is itself a negative value.
3) The existence of a negative value is itself a negative value.
4) The non-existence of a negative value is itself a positive value.

What is needed beyond this definition and axiology however is a deeper understanding of how values are perceived, how they interact with each other and how they thereby display nuances in their existence that are relevant for system design. Consider the analogy of the electricity domain: voltage, ampere and watt are different terms that mean different things. So just talking about "voltage" or analogously "values" does not suffice to properly acquire the domain for designing an electric device.

Material Value Ethics shows how a value is not just a (potentially theoretic) preference or opinion. In contrast and similar to geometric principles, values are *a priori given* (p. 135f in [13]), similar to what Plato called 'ideas'. A company CEO might hold the opinion that privacy is unimportant or outdated, but he or she cannot change the fact that the value of privacy exists in this world and that some users appreciate it.

This appreciation is always given as a *truly felt* preference. "We become aware of values in acts of feeling", writes Kelly [10]. But that does not mean that values are equal to emotion. Instead, the act of *value feeling* is the perceptual bridge to the higher conceptual phenomenon called "values", which cultures capture by *naming* them. For instance, one may feel good because a delicate message was fortunately encrypted. The related value here would be called 'privacy". Such naming of a value is a cognitive act that gives meaning to and retrospectively explains the emotion, feeling or preference at a more abstract level of reasoning. This process is relevant for value-based engineering, because potential system harms and benefits are often initially described by stakeholders in an unstructured emotional manner. Naming values adds the objectivity and justification to the design process that simple emotional reactions or fears are often lacking.

One might recognize that the encrypted message here was related to the value of privacy. But depending on context, encryption is often related to security as well. To be precise, Material Value Ethics would refer to encryption as *an innate value disposition in a system. which creates the potential for one or more values to unfold when using or examining the system* [p.79 in 11].[3] *Value dispositions are the technical or organizational prerequisites* created by engineers and the organizations they work for.

While value dispositions can be built into systems, values themselves cannot. Instead, values can only be „experientially present ‚on' the physical objects, acts, and persons we encounter..." (p. 19 in [10]). *This means that computer systems do not "have" values, but they "bear" or "carry" them if* they have the necessary dispositions built into them. For example, a full body scanner at an airport can bear the value of privacy if it has the technical disposition built into it that it represents people anonymously, processes their data securely, etc.

Finally, values are typically constituted by a multitude of *value qualities* in a context. The value of the security of a computer system is not only characterized by confidentiality achieved through encryption, but may also be driven by its integrity and availability. Therefore, it is more precise to say that multiple value qualities are actually instrumental for a value in a given context or can undermine it due to their absence. *Value qualities are the "real qualities of value itself"* (p. 6 in [11]) . *How value qualities actually manifest a value in a context becomes clear when comparing the meaning of a value such as security across contexts.* In a computer system the qualities of integrity, confidentiality and availability might be instrumental to security. On the other hand, take the value-example of "security" of a person on the run: The security of a person on the run would be affected by value qualities such as the secrecy of his/her whereabouts, the loyalty of supporters and the seclusion of the hiding place, etc. So the value of security takes on a completely different meaning due to its value qualities - secrecy, loyalty, seclusion. Still, in both cases the same value term "security" is used. Against this background we define a value quality in the context of a SOI, as the perceivable manifestations of a value that are either instrumental to it or undermine it.

Value qualities can be values in themselves or they are bearers of value. In any case, they form a kind of network structure around the core value they are instrumental to; thereby constituting the core value's meaning and manifestation in context. Kelly has nicely captured this dynamics when writing: *„...values condition each other, in that it is not possible, to grasp one value without having grasped some others."* (p. 11 in [10]).

For TM this dynamic is exemplarily depicted in figure 4 where the core value of equality (of patients) is characterized by a number of value qualities relevant in this context of the telemedicine platform. Equality of patients becomes meaningful when the positive value qualities of inclusion of the poor and access to the right specialists are granted. And it becomes meaningful when the negative value qualities of exclusion of non-computer users and loss of care in virtual encounter are avoided.

Taken together, we want to argue that the distinction of terms as they are elaborated in the philosophical literature are relevant for value-based engineering. They are captured in figure 1.

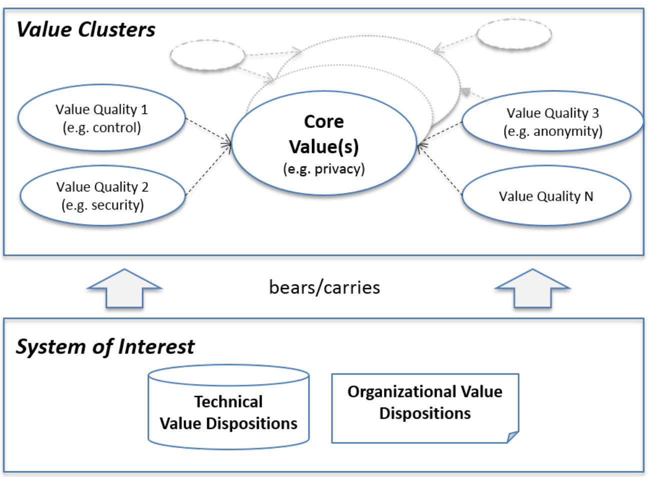

Figure 1: Value space phenomena and terminology

Recommendation 1: Working with values in computing should be accompanied by an awareness of the ontological differences between core values driven or undermined by value qualities and enabled by value dispositions, which are embedded in a system, which is a value bearer.

2) How can the ethicality of value-based systems be judged?

No matter how reasonable the value focus might be, the idea could not be taken for granted when VSD scholars first introduced it in the 1990s [16]. Human values will always remain contextually malleable phenomena of our "emotional intuition" (p. 272 in [10]), much more so than norms that are simpler, because repeatedly observable; or rights, which are articulated in the law. With values it seems as if VSD scholars introduced a "soft" element into the domain of engineering, which is a discipline more at ease with clearly definable and provable "hard" principles.

Quite a few values such as efficiency, dependability, or security have already gained their place in non-functional requirements engineering. Such technical values can be verified to some extent through "objective evidence" [17]. But many non-technical human values relevant for Ethically aligned Design are not as tangible, even if we clearly refer to them in our languages. For example, it is hardly possible to objectively measure the degree of loss of dignity an elderly person perceives if he or she is filmed in an embarrassing moment by a robot in a nursing home. And is this loss of dignity not a different kind of dignity than the kind of dignity hate-speakers lack when they bully others in alt-right forums? The example reconfirms that the meaning and importance a value changes from one context to the next and it may also be perceived differently in scale from one person to the next. Working with human values hence implies a readiness of the engineering community to work with a construct that is relatively fuzzy and malleable in its meaning and is difficult to measure, because it is contextually-situated and individually-specific. This is a challenge for those who prefer to trust only that which can be precisely defined and linear-causally determined [18]. Albrechtslund has called this challenge "the positivist problem" [19].

Since values are not objectively measurable, it is hard to proof at the end of an innovation project that the "value proposition" a system set out to create has actually been achieved. While user A might appreciate the control, transparency or privacy a system grants, user B might not even recognize any of these values as being present. Depending on our individual training, experience, preferences, etc. (or as Scheler calls it "milieu" [11]), we humans have varying propensity to perceive values. Therefore, the proof of a technical product being "ethical" can hardly be based on quantitative value judgments stakeholders make once a product is launched. Therefore, we recommend:

Recommendation 2: Stakeholder narratives and experiences should be used to gain insight into the success or failures of a value-based engineering.

That said, there is a second way to demonstrate that a system is good or ethical. This is due to the "act related values" inherent in engineering teams' and organizations' desire to create something worthwhile. As Hartmann outlines, "act values" [p.252 in 13] need to be distinguished from the values carried by artefacts themselves; so called "goods-values" [p.122 in 13]. Engineers deserve to be called "ethical" if they regard their systems as "value bearers" [p. 17, p.122, p.105 in 11] and then *genuinely intent* to create positive values (i.e. to create controllable, transparent and private systems) by embedding respective positive "value dispositions" into them (i.e. encryption) [11, p. 20]. Noting that there are also negative values, engineers equally deserve to be called "ethical" if they *genuinely intent* to avoid these (i.e. uncontrollability, intransparency, insecurity) and take the necessary precautions. If engineers act in this way, their work activity is ethical, because it is guided by their honest desire to do good. This intentional value cannot be taken away from them even if they fail to build a perfect system in the end. The value dispositions engineers build into their systems accompanied by the documented precautions they take, are an objective proof of their good intent. Therefore, value-based engineering is willingly transparent. It is rightfully proud on what it does and wants so show how technology is created for humanity. We therefore recommend:

Recommendation 3: The engineering organization should embrace a culture of openness, transparency and genuine care for doing good.

C. Preparing for value-based engineering

Value-based engineering can be engaged in at the very start of a new technology project (greenfield situation) or it can be applied to an existing service. In a greenfield innovation project, the starting point is an initial service idea combined with a first concept of operation. Such a concept of operation is a "verbal and/or graphic statement, in broad outline, of an organization's assumptions or intent in regard to an operation or series of operations" (ISO 1588). It roughly sketches out the envisioned "system of interest" (SOI), with its core elements, stakeholders, data flows, interfacing systems and context-of-use descriptions (see figure 3 for the TM case). In a brownfield situation this description is more detailed, containing the relevant existing system elements. In order to build a concept of operation the system boundaries need to be well understood as well as the degree of control an organization has over its service partners. Relevant stakeholders of the envisioned system need to be identified and involved. Most importantly, the deployment context of the SOI needs to be fully understood and ideally physically explored.

1) Recognizing ethically relevant system boundaries

When we hereafter speak of a "system" or "system of interest" (SOI), we always refer to a "socio-technical system". Systems that are defined as "socio-technical" regard technology as being embedded in organizational, public or private processes, or workflows with accompanying policies, people, preferences and incentive systems [69]. Compare this understanding of a system to the slightly narrower ISO 15288 definition of a system as a "combination of interacting elements organized to achieve one or more stated purposes" including „equipment, facilities, material, computer programs, firmware, technical documentation, services and personnel required for operations and support" [28]. In value-based engineering the system definition goes further and embraces more of the social aspects of a system. The method does not only consider the workflow system, its databases and interfaces and people working on these, but also the many stakeholders impacted by the system (including society at large) as well as the organizational processes, policies, work-modes and potentially culture surrounding the technical infrastructure.

That said, many systems today do not come as one clearly denotable socio-technical entity. Instead they are integrated into a wide network of systems; integrating for instance external web-services, databases and code components that originate from outside the organizational boundaries (third-party system). For example, when a SOI such as the TM integrates a video-chat application from an external service provider and stores patients' health data in an external cloud-service, there are effectively two external systems integrated into a SOI structure that presents itself as "one system" to end-users. The SOI is part of a wider "System-of-Systems" (SOS).

Such SOS can have a vital influence on the values created for end-users. If, for example, the cloud provider of TM does not handle the health data it stores in a secure and private way and gets hacked, patients will consider TM as untrustworthy no matter how private or secure TM's own internal systems may operate. SOI operators that pursue value-based engineering therefore need to stand in for the values of their SOS partners. We therefore recommend:

Recommendation 4: Value-based engineers should be ready to take responsibility for their whole ecosystem; at least for their first-tier partners.

In this vain, we are convinced that value-based engineering should require organizations to always include all those interfacing partners into their operational concept analysis that may have ethical import.

Requirement 1: Relevant first-tier external service partners must to be included in the operational concept description of the SOI.

This shouldering of responsibility is, of course, only rational if SOI operators have sufficient influence on what partners are doing. Value-based engineering therefore recommends in line with many experts a governance and control-analysis of all the elements of a SOI's SOS. The ISO/IEC/IEEE 15288 standard provides a framework to assess governance and control over a SOS. It recognizes virtual, collaborative, acknowledged and directed types of SOS [28].

Recommendation 5: A SOI operator should have acknowledged or directed control over SOS partners.

In acknowledged forms of co-operation, the constituent system owners retain independent ownership, management and resources, but they recognize joint objectives (i.e. value objectives) and designate a manager and resources to manage these objectives. Directed forms of co-operation go even further. Here, SOS are built and managed as one entity that fulfills a specific purpose and that is centrally managed. The component systems maintain their ability to operate independently, but the normal operational mode is subordinated to the joint and central purpose. In both of these forms of partnership the criterium for controllability is that the SOI operator can obtain access to the enabling system elements of the SOS.

2) Setting up a broad stakeholder group

Once it is clear hence who is technically and organizationally involved in a SOI, it is possible to complete the list of stakeholders. *Stakeholders in a value-based engineering effort are all those persons or entities who are impacted by the positive and negative value effects the system creates.*

Management guru Michael Porter once pointed companies to their responsibility to create "shared value" [23]; that is not only for their shareholders, but also for society at large. Two stakeholder categories are typically discerned: First, those who directly interact with a technology (direct stakeholders) and second, those who are affected by it but do not use it (indirect stakeholders) [2, 12]. Furthermore, Ulrich showed that the sources of stakeholder motivation, power, knowledge as well as their legitimation should be considered in their selection [24].

If stakeholders are those who are impacted by the value effects of the SOI then it is important that their values are understood. Scheler has described how ""striving after", „taking an interest in", „attending to", or „perceiving" some object takes place from within (a person's) milieu ... We can choose to act only on those things that can be effective upon us, that is, those that can attract our attention, arouse our desires, or move us to act" [10, p. 50]. Since a SOI is normally used by many different stakeholders, only an extensive and diverse stakeholder involvement has a chance to anticipate a relatively complete value spectrum at stake. In line with other scholars [2, 3, 5, 60], value-based engineering therefore requires:

Requirement 2: A wide stakeholder group must harvest their collective creative foresight of the SOI.

Many experts have been arguing furthermore that value-based engineering efforts should not shy away from including civil society representatives who sensitize for minorities and are critical of the SOI. This should include those who represent the interests of target market users. It is recommended:

Recommendation 6: Any international rollout of technology should be accompanied by the inclusion of stakeholders stemming from those world-regions, in which a system will be deployed and should equally be sensitive to minorities.

Once the right stakeholders are represented, Mingers and Walsham [25] have pointed to traits of "ideal speech situations" (building on Habermas [26]) to ensure that hierarchies and hidden agendas do not undermine an open discourse. Stakeholders should be allowed equal participation, encouraged to question claims and assertions and freely express attitudes, desires and needs [27].

3) Exploring the ethically relevant context

A fundamental challenge for Ethically aligned Design is that ethical behaviour is always deeply contextual. Even though Kant may have argued that it is one's duty to never lie regardless of context, history has shown that some situations may justify lying. Imagine a man in Nazi Germany who hid a Jew and opened the door to a Gestapo policeman asking for roomers. From a rule-based Kantian perspective the man should *not* lie [29]. But the true ethical challenge is that it could be seen as courageous and praiseworthy if he did. Lying could be the recommended behaviour by other ethical theories, such as virtue ethics or utilitarianism. In fact, it is the *context* that greatly influences whether a behaviour is right or wrong. Now imagine a humanoid household robot programmed with a Kantian duty ethical logic [29] was placed into a similarly dangerous political system in the future. It would open the door to a police officer and tell the truth, revealing a threatened group. Despite its moral algorithm, it might behave ethically questionable unless it would be sophisticated enough to understand its socio-political context.

The example shows that the context of a computer system's deployment must be deeply understood for it to behave well [3]. Noteworthy context elements in this example are the *political surrounding* in which the system operates, the *long-time horizon* assumed and the *infrastructure* available. VSD scholars have proposed to elicit values with scenarios and future-narratives that allow for inclusion of such context factors [2]. One of the VSD methods called "Envisioning Cards" [31] recommends to assume *pervasiveness* of a future system. Some negative values we see unfolding in today's digital services are only an issue because they have become so pervasive.

The pervasive computing community is working on properly conceptualizing context for applications that are prototyped and/or fully deployed here and now [32]. Common context factors include a user's location and environment, identities of nearby people and objects, and changes to those entities [33]. Many of these context categories can be associated with human values; often unveiled through ethnographic inquiries [2]. ISO/IEC 25046 includes a helpful common industry format for describing a context of use. However, it is only focused on usability and not ethicality of a SOI and it only looks at how user dispositions influence the SOI not the other way round that is the relevant one in value based engineering.

No matter how futuristic or timely engineers work and no matter what empirical method:

Requirement 3: A concrete context of use is the baseline for any ethical analysis and in its description it must be assumed that it is widely relevant.

For each reasonably expectable context of use the concept of operation contains the elements of a SOI, the data flows between these elements, the direct and indirect data subjects (stakeholders) involved and the data types processed. As Nissenbaum has argued: any system can be described in terms of these entities to capture what she coined "contextual integrity" [34].

The TM case can serve as an example: A generic videoconferencing platform with some adjunct databases and interfaces is deployed in a very specific health context here. Patients video-conferencing with TM doctors get immediate diagnosis, sick notes and referrals to specialists. TM wants to competitively differentiate itself through a database of highly-reputed specialists that patients can be referred to. This database is built up through a regular questionnaire-based inquiry among nationwide doctors. Here, *data subjects* (patients, specialists, recommending doctors and TM doctors) are profiled by the *data recipient* (TM) that collects various *data types*. One type is patients' medical histories. The other is recommendations from supportive doctors (*data senders*). The *transmission of the health data* is consent-based, confidential and commercial in the case of patients. And it is not consent-based, but confidential and non-commercial in the case of specialists that end up in TM's database.

The example illustrates the complexity of context modeling even for a simple system like TM's. Envisioning relevant values for all the involved entities in an concept of operation, recognizing different places of use, under varying political conditions, considering long-term pervasiveness, etc. is a mammoth task. Hartmann writes "…situations are of an individual nature, being only once and never returning." [13, p.13]. Therefore, engineers need to humbly embrace that the true future contexts of many of their systems can only be anticipated marginally. Only the real-world deployments and effective forms and places of later system use reveal the full spectrum of ethically relevant context-driven values that systems finally face. This again implies that initial value elicitation and prioritization for system design is not sufficient to ensure the long-term ethicality of a system.

Requirement 4: **O**rganizations must envision and/or explore the context of system-use not only prior to system design, but also update their context observations through ongoing monitoring of the SOI after system deployment with a view to adapting the system design accordingly.

This requirement is consistent with the iterative nature of the VSD approach as well as timely design thinking and agile forms of development.

Some experts recognize the fact that many systems today are initially of such generic nature that the context(s) of their later use are not known. For example, when computer vision algorithms are developed that translate a pixel space observed into a precise picture representation, then this kind of technology could be used in many contexts, ranging from cancer recognition applications to military drone targeting systems. Can such generic technologies already be engineered with values in mind even if the context of later use is unknown? Googles 'Project Maven' case demonstrated how engineers can be badly surprised if their generic technologies are (ab)used for instance for military purposes that some developers would not have wanted to support [35]. Against this background many experts argue that even for generic technologies it is a valuable exercise for engineering teams to reflect on possible future context scenarios. In most cases, grounded research has some kind of use case in mind when developing even highly generic technologies. Most importantly, however, there is a point relatively early in system design where a generic system is adapted to serve its final use. This is the point, for example, where the computer vision algorithm is applied to and trained with data from either a military or a health context.

Recommendation 7: It is recommended to begin with value-based engineering at that point where a generic technology is applied to a concrete use-context.

Here in can be most effective, because sufficient context information is known to think about the values involved and their ethical implications.

D. How value-based engineering works

If one discussed value-based engineering in relation to the traditional Waterfall SDLC (System Development Life Cycle), the core contribution of value-based work would be seen in the way by which it enriches the early phases of this traditional SDLC. These have been referred to as "IT project identification and selection as well as initiation and planning" [27]. The business literature also distinguishes this early phase of an innovation effort and has referred to it as the "discovery and scoping" phases [41]. In recent years, the term "design-thinking" has become popular in both disciplines [42].

Hereafter, we describe how three processes of value-based engineering cater to this early phase of system innovation: value elicitation, value prioritization and Ethcial Value Quality Drivers identification. These three processes constitute what we call the "Ethical Exploration Phase"; where "ethical" means "value-based". Once a company has gone through ethical exploration, it wants to ensure that those values it has prioritized and conceptualized are effectively finding their entry into the technical and organizational design of a SOI. An "Ethically Aligned Design Phase" takes care of this. It includes two complementary processes, a relatively light "Ethcial Value Quality Drivers Design Process" and a more time-consuming "Risk Assessment-Based Design Process". Both of them follow a risk logic: They foresee the systematic identification of treatments for relevant value threats. They differ, however, in their levels of depth, documentation and stakeholder involvement. Both processes end with the choice of system architecture and system design treatments. They differ in the rigor by which these treatments are prioritized, validated and monitored. Figure 2 summarizes the value-based engineering approach.

1) Ethical Exploration Phase

The ethical exploration phase envisions relevant human values associated with a SOI, it prioritizes and completes them in order to understand the goals of system creation, it shapes their role in the business mission, it anticipates ethical pitfalls and decides on further SOI investment. This phase of work should be supported by a *value-expert*, because some knowledge on values (i.e. a training in Value

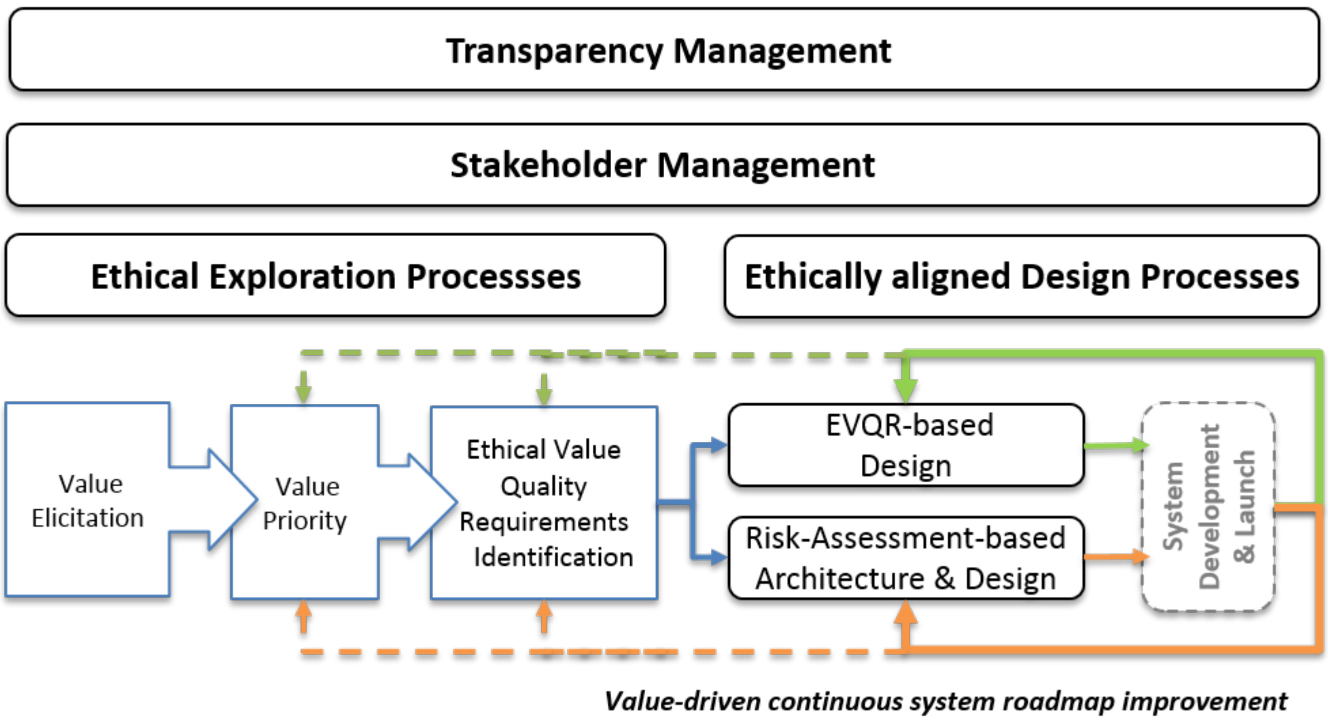

Figure 2: Process overview of value-based engineering

Ethics), a strong faculty of speech, an aptitude for conceptual thinking and system thinking, and also an understanding of the legal and technical "worlds" influencing the set-up of a system are required (see section 5 on the challenge of new roles and curricula).

Value Elicitation

Due to usability and user experience work the envisioning of values is not new to the HCI community. The value of usability for instance is related to joy, convenience, user control, etc. has radically transformed computer artefacts for decades. So, from a Material Value Ethics perspective the HCI community has always acted "ethically", because it genuinely intended to create system dispositions leading to the unfolding of these positive human values. VSD that evolved out of HCI has been driving this effort further by insisting that the deployment context studied should be sensitive to a wider spectrum of values, also values deemed important by indirect stakeholders or society at large. VSD has implicitly followed a Utilitarian philosophy that studies the consequences of actions [43].

Value-based engineering goes further: It explicitly requires to use the three grand ethical theories of the Western Canon for value elicitation: Utilitarianism , Virtue Ethics and Duty Ethics. Thereby it does not limit itself to an exercise of "moral imagination", but aims for "holistic value imagination", which means that stakeholders try to envision everything that might go wrong with the system and also all that the SOI could do good for the world in which it will become effective. Especially the latter envisioning of the positives has nothing to do with morals, but with positive visions for a technology-infused world. And it this positive envisioning that crucially distinguishes VSD from value-based design.

To be precise, value-based engineering efforts envision values with the help of three guiding questions [27]:

1. What are all thinkable positive and negative consequences you can envision from the system's use for direct and indirect stakeholders? (Utilitarianism)
2. What are the negative implications of the system for the character and / or personality of direct and indirect stakeholders; that is, which virtue harms or vices could result from widespread use? (Virtue Ethics)
3. Which of the identified values and virtues would you consider as so important in terms of your personal maxims) that you would want their protection to be recognized as a universal law? (Duty Ethics)

"Personal maxims" refer to subjective laws or principles of behaviour according to which a person thinks she *should* act; not because she is forced to, but because she believes in their virtue and fulfils a duty towards a "good" society by respecting them.

In addition to these three questions originating from Western philosophy it is sensible to consider a fourth question; one that embraces non-Western philosophical frameworks to elicit values, such as Confucianism or Buddhism. These cultural traditions have their own way to frame and ask for the ethical import of systems and can thereby shed light on different values that might not be captured by asking about consequences, virtues or personal maxims.

Requirement 5: To envision values the three grand ethical theories of the Western Canon for value elicitation must be used (Utilitarianism , Virtue Ethics and Duty Ethics) as well as any ethical belief system that might underly the culture where the SOI is going to be deployed.

When engaging in value-based engineering a number of noteworthy phenomena occur. When stakeholders and engineering teams envision values, they typically do not frame their thoughts in precise values. With a view to the TM platform for instance a stakeholder might say: "*What if patients are abusing the video chat with doctors and lie about their true condition just to get a quick sick leave note? Doesn't TM's virtual encounter encourage such lack of accountability*?" What this exemplary stakeholder reflection shows is that values need to be pulled out from what was said. In this case two values can be extracted: honesty and accountability. Accountability was directly named, honesty was hidden in the description.

What is more: some values keep coming back for a case in different disguises. In the TM case, for instance, privacy was an important issue. Stakeholders were reflecting on the degree of control they might want over their health data, the security of that data, and the positive potential to stay anonymous vis-à-vis TM doctors, etc. A value expert who is part of the engineering team would recognize that personal data control, security and anonymity are distinct value qualities that all relate to one underlying core value: user privacy. Core values, such as privacy in this case, keep coming back as important during value elicitation and they are constituted by multiple value qualities. Against this background we require to distinguish them:

Requirement 6: For each SOI context core values must be distinguished from their value qualities.

What is practically useful is to speak about the creation of "value clusters" when value experts group core values with their value qualities (see figure 4 as an example). As part of this clustering work, the value experts name value qualities which stakeholders might have only described indirectly. Thereby, he or she benefits from system ideas stakeholders might have mentioned for the concept of operation. It is not unusual that in the midst of thinking about a value like privacy a TM stakeholder would for instance suggest to encrypt the health data. Such ideas are invaluable: They should not only be collected for later system design and subsequent improvement of the SOI sketch, but they help the value expert to better understand and complete the value qualities that stakeholders meant to express.

Recommendation 8: Clustering core values and value qualities should allow for the facilitation of value prioritization

In TM's case, 93 values were directly or indirectly mentioned by stakeholders and it would have been impossible to put these in order for syst3em design. Therefore, value experts grouped these into 93 in 13 core value clusters with respective value qualities. Some of this analysis is captured in the case study below. A detailed description of this can be found in [65].

Value Priority

Once core value clusters are identified, engineering teams need to decide how these should be prioritized. Value based engineering recommends the involvement of corporate leaders in this prioritization to avoid later value conflicts among engineers during development [1].

Recommendation 9: Not only engineers, but also corporate leaders and a wide group of stakeholders need to be involved in value prioritization.

Three complementary analyses are recommended to prioritize core values: The first investigates how core values resonate with the existing or emergent business mission. The second analysis is a duty ethical one. And the third analysis requires organizations to check core values against existing corporate principles, legal frameworks, international human rights agreements or relevant ethical principle lists. If values are missed in the value elicitation process, they can be added; potentially even as a priority.

For TM, the first business-oriented analysis showed that out of the 13 core values identified for its platform it would be well advised to either focus on patient comfort, patient equality or on doctors' knowledge creation. It was the choice between these three very distinct core value foci or "value propositions" that would lead to a completely different priority ranking of the other core values relevant for the system (see table 1). TM's CEO decided to prioritize the value of equality. He made this choice in line with the corporate mission he had pursued from the start of his business - that is giving everyone access to a good specialist. Examples for corporate principles beyond the TM case are IBM's commitment to accountability, explainability and fairness of its products [46], or Microsoft's commitment to people empowerment, community and environmental sustainability [47]. Such duty principles show their ethical worth when they are used to effectively guide system design's value priorities.

One of the grand rules of duty ethics is Immanuel Kant's Categorical Imperative reads: "Act only in accordance with that maxim through which you can at the same time will that it become a universal law" [29, p. 73). When corporate leaders are involved in value prioritization, they should query these personal maxims they hold. Value-based engineering requires them to consult themselves and support only those value principles that they would want to become universal. Moreover, the second part of the Categorical Imperative asks them to never treat other people as "a means only" to achieve their goals. So if for instance a service is created primarily to create profit from selling customer's personal data, then customers are used as a means only to serve financial gain. Value-based engineering would consider this an unethical prioritization of value. A 'higher' value, such as customer joy, or customer knowledge must be prioritized for system design in order to create technology for humanity.

A challenge that can occur at this point is that values sometimes contradict each other and require engineers to make a choice for one or the other, always losing out on some value. This mutual exclusion of values is often seen as a dilemma. Material Value Ethics provides for a hierarchy of values and claims that ethical behaviour is constituted by choosing and realizing higher values over lower ones [10, 47]. Scheler described how the relative endurance, deepness and indivisible nature of values are criteria for their superiority; their relative independence from value bearers and the degree of intrinsic value they have are also a sign of their "rank" [11, p. 86ff]. Taking two values from TM's case can illustrate this. Today's active benevolence among doctors that is born by the activity to recommend each other may be traded in with efficiency born by a database. Efficiency however is a lower value. Unlike benevolence, it has little intrinsic value. One can ask: "What is efficiency good for?" and debate that sometimes – for instance, in human relationships - efficiency is not good. True benevolence would not be doubted as worthy in itself. Benevolence leads to deeper satisfaction in people than efficiency does. So the great metaphysical value conflict TM confronts is that it may promote a value of lower priority if it subsumes benevolence to efficiency.

No matter what the specific value constitution may look like, one value most praised today by corporate management and financial markets is that of profit. Even though profit is a low value according to the rank order of Material Value Ethics, managers are under pressure to make profit for shareholders. Instead of following their moral intuitions, intentions, duties or objective value hierarchies, they might be tempted to downplay values, such as benevolence, and prioritize efficiency or profit instead. This is a threat to value-based engineering.

System experts have been suggesting a number of provisions that can be made for good choices: First, as we will show below, value-based engineering requires transparency. It asks for binding value priorities to individual executives who have to personally sign and openly stand in for their decisions. Furthermore, it is recommended that the wide group of stakeholders described above should by and large support the prioritization process. The final decisions on value prioritizations should not be taken only by top-executives' 'brute force' and without the support of the stakeholder community involved. Feedback cycles from end-customers of the service are required once a service is launched. Such feedback supports the continuous improvement of a system so that value priorities can mature as the system matures. Finally, it is recommended that companies do not fully decide the value list for themselves. Experts agree that companies should check target market regulation and international human rights agreements for ethical principles a company should respect as well as ethics guidelines. Legally recognized ethical principles provide the outer boundary condition for corporate action and should impede some prioritization of negative values.

Taken together, the following recommendations and requirements result:

Recommendation 10: Corporate leadership should personally sign and openly stand in for a SOI value priorities and related decisions.

Recommendation 11: A majority of stakeholders should support the value prioritization made.

Recommendation 12: Regulations and human rights should be consulted for the prioritized value list compilation.

Requirement 7: Feedback cycles on value priorities with end-users of the service are required once a service is launched.

The reflection of duties, corporate and legal principles as well as value hierarchies should lead innovation teams and leaders in some cases to decide against investment in a new product or service This decision to not invest must be seen as a critical part of value-based engineering. Value-based engineering is not only about value elicitation and prioritization, it is also about an ability to forgo business opportunities and profits that disrupt society and/or human wellbeing. An Ethically aligned Design is senseless if more negative value than positive is created.

Ethical Value Quality Driver Identification

A vital part of ethical exploration that has already a tradition in VSD is the *conceptual analysis* of values [2]. After core value clusters have been prioritized, organizations need to ensure that their core values and respective value qualities collected bottom-up from stakeholders are conceptually completed as far as this is possible. For example, the core value of privacy might have been characterized for TM's case in terms of patient's health data control, data security and the possibility to stay anonymous as a patient. But with these three value qualities alone, the core value of privacy is not yet sufficiently captured. What constitutes the value of privacy from an expert perspective is for instance additionally described in the General Data Protection Regulation (GDPR) [48] or in court-decision reviews of privacy harms [e.g. 6, 49]. Such external sources provide a refined view on the value qualities that need to be in place. For the core value of privacy, for example, qualities such as data portability, data accessibility, data quality and the assurance of legitimacy of any further health data use will play a role. Value-based engineering therefore requires that a conceptual analysis is conducted. In value-based engineering this is a hermeneutical exercise, which completes and refines the bottom-up collection of core value qualities. For this purpose, value experts should consult legal texts, but also philosophical, technical or managerial ones.

Once this completion is assured *Ethical Value Quality Drivers* (EVQDs) can be derived from each value quality. The use of product *drivers* for technology roadmapping is borrowed from Lucent Technologies at outlined in (x); only that drivers in value-based engineering are explicitly linked to human values rather than being drawn from competitive analysis or technology availability. *EVQDs are the tangible organizational or technical measures catering to the value qualities that stakeholders and conceptual analysis identified as relevant for the SoI.* Taking the value quality of 'informed consent' in TM's case as an example, the EVQDs might include [50]: (1) meaningful and comprehensive descriptions of personal data processing activities to TM users, (2) truly voluntary obtaining of their consent, (3) easily accessible options to decline consent and (4) measures to avoid consenting to something one does not understand.

The chain from core values to value qualities and to EVQDs should be traced by organizations in what we call a "Value Register"; i.e. with the help of a numbering system. This helps to ensure that system design will later systematically cater to values and that the ethical thought process is comprehensive. In this Value Register, an EVQD like informed consent might be described with adjectives like "meaningful", "comprehensive" or "voluntary". But the question is what this means and what minimum threshold levels or performance outcomes are actually necessary for an EVQD? It is therefore recommended to add such threshold levels to the Register to later check whether the system lives up to the EVQDs in a satisfactory way. Why such threshold determination is important becomes clear when looking at the miserable way in which many European companies today fail to live up to the EVQD of informed consent (required by the GDPR). Many continue to inform their users of personal data collection through lengthy legal text that laypersons can hardly understand. Many nudge users into consent i.e. by covering half of the user screen with consent forms that do not go away unless the user agrees to personal data processing. Unless an organization agrees on minimum EVQD fulfilment standards with its stakeholders, risk remains that some will minimize later ethical design efforts.

Taken together value-based engineering foresees the following recommendations and requirements to identify EVQDs:

Requirement 8: The value qualities instrumental to or undermining a core value in a context need to be hermeneutically completed and refined in a conceptual analysis.

Requirement 9: Ethical Value Quality Drivers (EVQDs) must be derived for each value quality.

Recommendation 13: Value qualities, EVQDs and their thresholds should be agreed upon by the stakeholders and entered into the Value Register.

2) Ethically Aligned Design Process

Methodologically, value-based engineering strives to ensure that all *value quality r*equirements are finding systematic entry into the system design. Therefore, the system design process needs to ensure that they are translated into concrete *system* requirements.

Remember, system design here means 'socio-technical' system design and therefore includes not only technical measures organizations can embrace, but also organizational ones. People, policies and management can probably address many EVQDs at the organizational level without any technical dispositions built into the system. For example, if TM's mission is to foster more equality in the medical system and to help non-insured patients to get treatment of recommended specialists, then it first needs to motivate such specialists to open their offices for this kind of care for the uninsured. After all: who needs a specialist database and recommender system if patients cannot get an appointment with the doctors they are referred to? That said, many value qualities and their EVQDs will need to be addressed by the technology design or technology-related policies.

As outlined above, value-based engineering has two complementary process approaches to design a system: One is a lighter iterative EVQD Design Process that has commonalities with the classical design thinking or agile approaches to system design. For all EVQDs that organizations have the power to address, it is required that they run through this EVQD-based design process *unless* the value quality the EVQD caters to is of such scale and importance for human wellbeing, mental or physical health or life that a deeper Risk-Assessment based Design Process is necessary. Also when value qualities are legally recognized as important they should undergo Risk-Assessment based Design.

Requirement 10: Depending on the legal, mental/physical health and life impact of a value quality, the decision must be taken as to whether it needs a rigorous risk-assessment based system design approach for requirements engineering or whether it is fine to address it through an ordinary, lighter risk-based design process.

Light Risk-based Design

The Light Risk-based Design Process can be conducted by pursuing four tasks: First, the project team develops what usability experts call "personas" [27, p.221f]. In classical system design personas are descriptions of archetypical direct end-users of systems. They act as stand-ins for real stakeholders**.** In value-based engineering indirect stakeholder personas are recommended to be also included.
In TM's case, for instance, the doctors that recommend other doctors should be represented by a persona whose interaction will be simulated to explore in what form specialist advice should or should not be given.

Second, EVQDs are analyzed with regard to whether personas would perceive them as threatened. And for each threat, concrete system requirements are derived to mitigate and control these threats; including architecture related requirements; we call these "value-risk-control requirements"

In a third step, these value-risk-control requirements are used to inform system mockups or prototypes, which are iteratively tested with real internal and external stakeholders. What is important here is that prototypes can often not be exclusively based on value-risk-control requirements. Instead, value-risk-control requirements need to be integrated with other (mostly functional) system requirements that are not stemming from the ethical thinking process described here. Many organizations for instance may have existing technical systems and want to improve them with value-based engineering. They might want to make an already existing technology fruitful for their business. Or they are faced with external business requirements that lead to specific business expectations on the SOI that are not derived from any ethical value reflection. These externally given (mostly technical) system requirements must be integrated with the value-risk-control requirements in what we call a *"holistic system concept"*. This holistic system concept embedded in system mock-ups or prototypes should live up to the agreed EVQD threshold standards.

In the fourth step, the most promising holistic system concept enters the test market where real-world feedback is gained. In design thinking the term "first viable product" is often used. It is recommended that continuous feedback is collected on this and later viable product versions; a feedback that may complement the value qualities, EVQDs or even core values and their priorities successively. So the theoretical value exploration phase now becomes a life-exploration phase that iteratively circles with the Design Process to continuously improve the SOI.

With this approach, EVQD-based design monitors the evolving system not only with regard to system functionality, usability, etc., as is often done today. Instead, it includes the monitoring of the positive and negative values unfolding. It looks at whether the value-risk-control requirements are met. Users can put systems to unethical uses not anticipated or systems can produce unexpected negative values, such as addiction, hate or long-term unease. That is, negative values that were not foreseen can appear. Such values would then be re-inserted either into the value prioritization activity described above or be added to the EVQD identification process. Also, it might turn out that protection against anticipated negative values is not as successful as planned. EVQD-based Design includes the monitoring of how the treatments chosen are effective in mitigating value threats later.

Light Risk-based Design recommends and requires the following:

Requirement 11: In a Light Risk-based Design Process value risk control requirements are identified based on threats to EVQRs.

Recommendation 14: Personas can be used to model the perspective of direct as well as indirect stakeholders to identify the value risk requirements in line with their expectations..

Recommendation 15: After service launch, constant market feedback should inform further product iterations and complement EVQDs, value qualities, core values, stakeholders and value priorities.

Risk-Assessment based Architecture and Design

While the Leight Risk-based Design Process will be sufficient to address many EVQDs, some value qualities are so vital for stakeholders that system design needs to be even more rigorous. In such cases it is more difficult to integrate already existing or external system elements or functional system requirements that have not been developed with a risk logic in the first place. It is necessary that organizations build their SOI from scratch and potentially migrate existing systems into the new risk-aware infrastructure.

Risk-assessment based design methods are well established for some values, such as security, privacy or safety [74]. However, there has not yet been an attempt to generalize these methods to a generic value level. This is necessary for value-based engineering. In a nutshell, risk assessment-based system design as translated from privacy-risk assessment (x) would start out from the value quality and its EVQDs. For each EVQD the first step is to investigate its level of protection demand by asking what would happen to various stakeholders if the EVQD was not met? This question can help to weigh the EVQDs level of protection demand; normally on a nominal scale. Afterwards, each EVQD undergoes a threat analysis. While in security and safety assessments this threat analysis comprises a calculation of threat probability, many human value threats might not be that easily quantifiable. Therefore, it should suffice to judge whether a threat is realistic or not. And for those that are, each one needs to be addressed and mitigated by a respective system control. System controls can be functional, non-functional, operational, procedural, organizational or structural requirements. However, there are typically several control options available at different degrees of rigor. The choice of the right value-risk control requirement with the appropriate rigor should be informed by the level of EVQDs respective protection demand. Other authors have referred to this as the choice of the right "degree of stakeholder *exposure*" an organization is willing to accept [3].

It is recommended that the whole process of deriving control requirements is documented and traceably linked to the respective value qualities. This ensures the demonstration of the "act value" that engineers are bringing in. The effectiveness of the controls chosen should then be monitored during market deployment and adapted throughout the life cycle of the system. The latter might be done by that party which continues to service the system.

Requirement 12: In a Risk-assessment based Design Process value risk control requirements are traceably identified. This is not only done with the help of a threat-control analysis, but also on the basis of the level of protection demand identified for EVQD.

3) Transparency management for ethics by design

Genuinely intending and creating value dispositions in products has been described above as a core ambition of value-based engineering. The value that lies in this form of activity needs to be appreciated in itself. Therefore, the artifacts produced in each process described above should be documented. We therefore recommend:

Recommendation 17: An Ethical Registrar should accompany the ethical exploration phase as well as the risk-driven design phase.

The Ethical Registrar can serve project management and later auditors to recap at any time what the goals of the project were, who was involved and who signed responsible for it.

In addition, it is recommended that an *Ethical Policy Statement* is made publicly available. Here senior executives shortly explain the prioritized core values of a new system and demonstrate how these were recognized in practice (for example in the appendix of the annual corporate report). It is helpful to simply take the prioritized list of core values and formulate the Policy Statement around these core values (see case study).

The Ethical Register should contain the full spectrum of conceptually analyzed core values and value qualities depicted in their clusters, ideas for the concept of operation that were captured as well as the priorities agreed on. The stakeholders involved should also be noted as well as their agreement and disagreements on individual value qualities and EVQDs. The names and personal signatures of those top-executives who take personal responsibility for the priorities and the risk strategy chosen must be captured (see: Recommendation 10).

The documentation effort has of course the disadvantage of costing extra time and effort that is not en vogue in times of low-cost and agile system development. However, there are two key advantages of documenting these information items beyond validation. First, it is possible to develop a culture of responsibility and transparency that is at ease to tackle things that go wrong. Take the case of Volkswagen where the culture was not as open and where it took months to understand who took the decision when and in what context to build misleading software for the cars' emission statistics [51]. Such lengthy searches for culprits and scapegoats are traumatizing engineering departments and anyone involved in a respective innovation effort. And secondly, one should not underestimate the power of the performative act that goes in line with putting one's name down in person. The performative act of standing in for something in written form is likely to foster accountable behavior and supports more appropriate risk taking. When no one wants to put down his or her name for a system design choice or value priority, then this is also a good indicator during engineering for re-thinking a respective decision.

E. Challenges for value-based engineering

It is clear that value-based engineering is not an easy endeavor for companies. In many respects it implies a new way to think about systems' mission, a new way to build them and an embracing of a careful and highly controlled engineering culture in computer science. Besides this overall challenge and the cost it implies, we foresee at least four major challenges: The first challenge is one of corporate responsibility and co-operation. The second challenge is the need for new roles; especially the education of values experts. The third is a more careful use of agile forms of system development that are currently so much embraced. The fourth challenge is that organizations need to resume responsibility and control in widely interconnected SOS environments. And the fifth one is that ethical truths are difficult to swallow for entrepreneurs and innovation teams who might be enthusiastic about a technology potential that they really should not pursue or pursue in a way they would prefer to.

1) A willingness to be responsible

Value-based engineering requires an evolution of software engineering culture towards ethical diligence. While agile forms of software engineering have been heralded in recent years as a breaking free from rigid and reporting-loaded and process driven work [21], leading to rapid results [52], ethical engineering requires some back-pedaling. Time must be taken to think about value requirements, risk management and to write the necessary documentation. This time is often not part of the budget plan. Technical engineers also got used to delegating much of the ethical responsibility to legal departments [53, 54]. About 40% of them do not feel responsible for instance for the privacy and security of their systems [75]. They would now need to tackle much more of the ethical implications of their work and closely co-operate with product managers who are responsible for the non-technical, organizational precautions of an ethical service. Such co-operation between engineers and managers has proven difficult in the past, because management and engineering departments have very different work cultures [27].

2) New Roles and Training Curricula

As was shown above, the value exploration phase needs a new kind of employee: A value expert. People with this job and personality profile need to have a faculty of judgement that can be obtained from interdisciplinary education or coaching that is still rare today; knowing the humanities with a focus on ethics and values and having a good understanding of technology and management as well.

Ideally, value experts should *not* be independent consultants who leave a project once a first system version is deployed. Since there is iteration and monitoring foreseen as part of Risk Management a person permanently embedded in the development team should be embracing this role; for example someone who has the longer-term 'power user', 'scrum master' or 'system engineering' role in development efforts or who is the permanent product manager of the system.

The investments into new roles and responsibilities, diligent engineering processes, etc. need to be shouldered by entrepreneurs or organizations that are now used to highly agile work styles, rapidly releasing services early and often, outsourcing many practices, etc. There are two challenges for value-based engineering that are of particular importance: One is the way software innovation is created today. The other is a business environment, in which data-driven business models push companies into ethically questionable practices of work [55].

3) A re-embracing of control and accountability

As was outlined in this paper, value-based engineering seeks a high degree of control over engineering artifacts: the eco-system of partners needs to be accessible and manageable, value qualities are all traced to end up in concrete socio-technical measures, etc. This culture of control-based responsibility is challenged by the way software is built today. Especially smaller companies tend to copy requirements from established applications [56], leading to a progression of biases [57] or other unethical requirements. Furthermore, today's software is often build out of pre-developed functional modules. Less than 30% is custom-built [35]. Such modules, however, are often proprietary, not allowing in-depth investigation, or engineers might lack the special knowledge necessary to fully assess them. A related challenge is that modern software is very complex and consists of many functionally linked modules, which can cause unpredictable interactions. This potential for unpredictable interactions makes upfront planning very difficult and time-consuming [35]. Often, modules are closed source or so called proprietary system elements and require highly trained engineers. Take again the case of TM that just has a five people budget and needs to integrate third-party video-conferencing software in its service if it ever wants to go life. It cannot control the security level and data-handling policy of its video-software partner. Even if TM found an appropriate partner, the next question is how it can make money. In today's data-driven digital economy, the company is almost forced to play with the idea to sell its patient diagnosis data at some point, considering it as a valuable source of profit. The ethical necessity to forgo at least involuntary forms of secondary patient data usage is not easy for such a small company. It would then depend solely on its service quality, which may be the right way, but not one desired today by many investors.

4) Readiness for one's ethical truth

Finally, value-based engineering demands a high level of personal maturity from everyone involved in it. As the authors learned from the TM case study, being confronted with the negative values one might create is psychologically difficult for managers who want to succeed with their idea. We "tend to adjust our value judgments to our factual willing and acting (and our weaknesses, deficiencies faults, etc.)", wrote Scheler about the challenge to truly face the values one creates [11, p. 327]. In TM's case, the CEO needed to face that he might be breeding distrust, envy and competition among doctors if his service ever reached a relevant market share. The message that TM might exchange a culture of benevolence with a culture of efficiency is not a message that goes down easily. And it might only be in the earliest phases of system design that such openness exists; a point where the value proposition or mission can still be changed. Or, a company needs to be in a situation of such ethical turmoil that it is ready to radically turn around its business with value-based engineering, regardless the changes and costs to the business model and technical infrastructure.

So taken together, value-based engineering presents a deeply reflective, challenging, time-consuming and diligent way to build and run ethically aligned technical products and services.

F. Case Study

The Telemedicine start-up (TM) initially started with the classical product roadmap planning [58, 59] whereby it identified 12 typical business values: It stressed efficiency, convenience and flexibility for patients and doctors due to less physical encounters. It saw a health improvement for patients due to specialist recommendations as well as linked insurance cost advantages. TM also recognized that health data would need appropriate security and privacy measures. Figure 3 shows the concept of operation of TM.

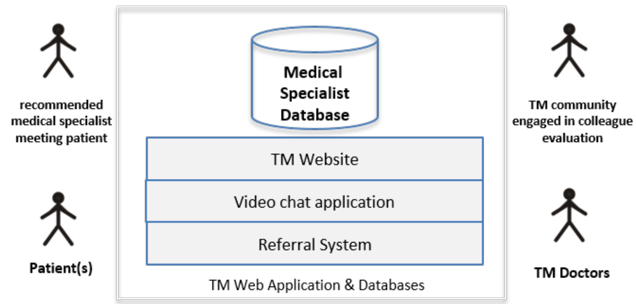

Figure 1: Rough concept of operation overview of TM

TM then engaged in value-based engineering with the authors of this paper. 19 pairs of students enrolled in an Innovation Management class of one of the authors and were introduced to the concepts of value-based engineering and the three ethical questions. They consciously reflected on all relevant direct and indirect stakeholder perspectives under the assumption that TM would become a leading national provider of telemedicine services.

Value Exploration: Students identified 7 stakeholders and 93 core values as opposed to the 12 values embedded in the CEO's original product description. They saw TM's business values materialize very differently from what the company thought: They argued that TM only has a fragile potential to improve the *health* of patients. This health potential depends on the *sustained benevolence* of the medical community, which needs to be willing to continue providing 'objective' and honest specialist recommendations for TM's specialist database. This benevolence is at risk though, because mutual ranking and rating of colleagues can breed *competition among doctors*, *greed* and *dishonesty*. The TM platform can also breed *dishonesty among patients* who might abuse the service for quick referrals, medication or sickness notes. TM also has the potential to *undermine health*, because diagnosis requires the human touch and TM has to find a fine balance between the digital shortcut and the analogue virtue of doctor-patient encounters. The *efficiency* aspect of the telemedicine platform bears the challenge that *trust and patience* between doctors and patients is undermined and today's respectful relationship is exchanged with the *commodification of a discipline*. *Privacy* can be fostered by TM, because it allows shy patients to remotely access medical advice in delicate affairs. As far as the *fear of 2ndary data use or abus*e of medical data is concerned, however, it is less the hygiene factor of data encryption that matters (which TM had foreseen), but the *transparency* required from TM's business model of how patient data is dealt with

Value prioritization: Besides the value of health that is the obvious overarching value catered to in this case study, 12 core values could be identified with respective value qualities. The core value later prioritized by TM is the *equality* in medical service. Even elderly or handicapped people who cannot visit a doctor anymore can be serviced through TM (value quality: inclusion). This is only offset by the exclusion of those who do not want to use a computer (negative value quality). Anyone can get good referrals to specialists they would otherwise not know about (value quality: access). A negative aspect of this form of equal virtual treatment is a likely loss of care (negative value quality). Due to the virtual encounter, patients are less encountered by doctors in their uniqueness. Figure 4 illustrates the value cluster for the core value equality with its positive value qualities of inclusion and access and its negative value qualities of exclusion and loss of care.

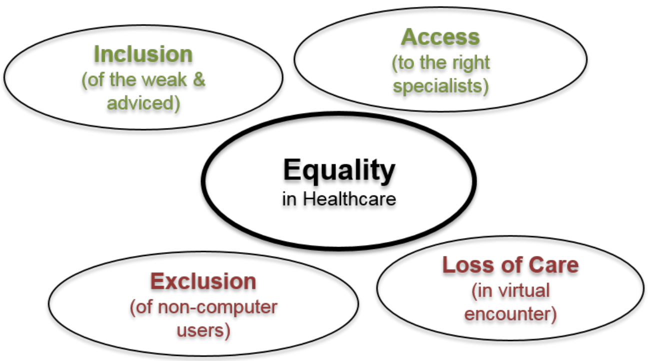

Figure 4: Value cluster for the core value of equality

Another business opportunity for TM would have been to become a *knowledge* platform for doctors. Doctors could virtually support each other's diagnoses in difficult cases and thereby foster *co-operation* and *life-long learning in community*. Such a usage of the platform would have supported the long-term benevolence TM needs from the medical community. Mutual referrals would have been a natural result of an online community of specialists and doctors supporting each other. A third core value priority could have been *comfort*. TM would have become the most convenient first-tier doctor encounter that replaces some of the physical visits today. Table 1 illustrates how the value mission changes the prioritization of core values.

Equality Mission	Knowledge Mission	Comfort Mission
Equality	Knowledge	Comfort
Trust	Reliability	Trust
Accuracy	Accuracy	Safety
Reliability	Privacy	Privacy
Honesty	Trust	Patience
Privacy	Honesty	Honesty
Safety	Equality	Equality
Fairness	Efficiency	Knowledge
Efficiency	Patience	Accuracy
Comfort	Comfort	Reliability
Patience	Safety	Efficiency
Knowledge	Fairness	Fairness

Table 1: Change of value mission

This prioritization is not necessarily based on any measurable judgements, but on the corporate principles, qualitative stakeholder and leadership views and the duty ethical reflections outlined above. Note that the value of privacy is listed only as rank six for the prioritized equality mission. This ranking position would need to change according to IEEE P7000 because privacy is a value highly regulated and must be considered as a hygiene value with at least second highest priority for an ethics by design.

Based on this prioritization, the Ethical Policy Statement of TM could read: "The Company TM's core goal is to create a recommendation platform for specialist doctors that is maximally inclusive for any patient, ensuring that anyone has access to the right specialists. TM cares for the privacy of the patients it interacts with and wants to foster trust, honesty and accuracy on its platform thereby creating a perception of safety in people needing help."

Value Conceptualization: The prioritized values will need to be conceptually completed and broken down into ethical system level value quality needs, EVQDs. For each of these it will then need to be decided what further design process is appropriate. Equality in the way TM wishes for is not regulated in any international agreements; nor will the EVQDs relevant for equality threaten the life or health of patients. Therefore, the EVQDs related to equality will need to undergo only a Responsible Design Process (see table 2). However, other value qualities, especially those related to privacy, will need to undergo rigorous risk assessment for proper design derivation.

Core Value	Value Quality	Ethical Value Quality Requirement (EVQD)
Equality	Patient Inclusion	Avoid discrimination of any patient by binding TM's use to undesirable outcomes.
		Avoid denial of opportunity of TM service usage.
		Exclude patients only on reasonable and appropriate grounds.
		Avoid any systematic exclusion of individuals or groups from TM.
	Specialist accessibility	Integrate only specialists who are willing to accept any patient.
		Develop programs for allowing conditional access.
	Lack of patient-doctor care/virtuality	Allow for care to unfold.
		Avoid to display any biased patient data.

Table 2: Technical & Organizational EVQDs for Equality

Acknowledgment

The authors wish to thank participants of the IEEE P7000 working group for their time and effort to participate in more than 80 calls over the span of almost four years to discuss the matters described in this article; especially Ali Hessami, Lewis Grey, Ruth Lewis, Annette Reilly, Gisele Waters, Jake Metcalf and Alexander Novotny. We want to thank the CEO of TM for the opportunity to do the case study. We want to thank our colleague Kathrin Bednar for her value expert work to build the case study.

References

1. Shilton, K., *Values Levers: Building Ethics into Design.* Science, Technology & Human Values, 2013. **38**(3): p. 374 -397.
2. Friedman, B., Hendry, D. G., & Borning, A. (2017). A survey of value sensitive design methods. Foundations and Trends® in Human–Computer Interaction, 11(2), 63-125.
3. Robertson, L. J., Abbas, R., Alici, G., Munoz, A., & Michael, K. (2019). Engineering-based Design Methodology for Embedding Ethics in Autonomous Robots. Proceedings of IEEE, 107(3), 582-599.
4. Johnson, D.G., *Computer Ethics - Analyzing Information Technology*. 2009, New Jersey: Pearson International Edition.
5. Frauenberger, C., Good, J., Fitzpatrick, G., & Iversen, O. S. (2015). In pursuit of rigour and accountability in participatory design. International journal of human-computer studies, 74, 93-106.
6. NIST, *NIST 800-53: Security and Privacy Controls for Federal Information Systems and Organizations*, N.I.o.S.a. Technology, Editor. 2013, U.S. Department of Commerce: Gaithersburg, MD.
7. Oetzel, M. and S. Spiekermann, *Privacy-By-Design through systematic privacy impact assessment – presentation of a methodology.* European Journal of Information Systems, 2013. **23**(2): p. 126-150.
8. Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. Nature Machine Intelligence, 1-11.
9. Kluckhohn, C., *Values and Value-Orientations in the theory of action: an exploration in definition and classification*, in *Toward a general theory of action*, T. Parsons, E.A. Shils, and N.J. Smelser, Editors. 1962, Transaction Publishers: Cambridge, Massachussetts. p. 388-433.
10. Kelly, E., *Material Ethics of Value: Max Scheler and Nikolai Hartmann*. Phaenomenologica, ed. Husserl-Archives. Vol. 203. 2011, Heidelberg London New York: Springer.
11. Scheler, M., Formalism in Ethics and Non-formal Ethics of Values: A New Attempt Toward the Foundation of an Ethical Personalism. Northwestern University Studies in Phenomenology and Existential Philosophy. 1921 (1973), USA: Northwestern University Press.
12. Friedman, B. and H. Nissenbaum, *Bias in Computer Systems.* ACM Transactions on Information Systems, 1996. **14**(3): p. 330-347.
13. Nicolai Hartmann. Ethics. 4. Auflage, de Gruyter. Berlin. 1962.
14. Vallor, S. (2016). Technology and the Virtues - A Philosophical Guide to a Future Worth Want-ing. New York: Oxford University Press.
15. Malle, B. F., Scheutz, M., & Austerweil, J. L. (2017). Networks of social and moral norms in human and robot agents. In A world with robots (pp. 3-17). Springer, Cham.
16. Rogerson, S., & Gotterbarn, D. W. (2005, January). Responsible risk analysis for software development: creating the software development impact statement. AIS.
17. ISO 9000:2015, "Familiy - Quality Management", Internet: https://www.iso.org/iso-9001-quality-management.html, Oct 2019.
18. Manders-Huits, N. (2011). What values in design? The challenge of incorporating moral values into design. Science and engineering ethics, 17(2), 271-287.
19. Albrechtslund, A. (2007). Ethics and technology design. Ethics and information technology, 9(1), 63-72.
20. Davis, J., & Nathan, L. P. (2015). Value sensitive design: Applications, adaptations, and critiques. Handbook of ethics, values, and technological design: Sources, theory, values and application domains, 11-40.
21. Manifesto, A. (2001). Agile manifesto. Haettu, 14, 2012.
22. Sillitti, A., & Succi, G. (2005). Requirements engineering for agile methods. In Engineering and Managing Software Requirements (pp. 309-326). Springer, Berlin, Heidelberg.
23. Porter, M. and M.R. Kramer, *Creating Shared Value.* Harvard Business Review, 2011. **89**(1).
24. Ulrich, W., *Reflective Practice in the Civil Society: the Contribution of Critically Systemic Thinking.* Reflective Practice, 2000. **1**(2): p. 247-268.
25. Mingers, J. and G. Walsham, *Toward Ethical Information Systems: The Contribution of Discourse Ethics.* MIS Quarterly, 2010. **34**(4): p. 833-854.

26. Habermas, J., *The Theory of Communicative Action Vol 1: Reason and the Rationalization of Society*. 1984, London: Heinemann.
27. Spiekermann, S., *Ethical IT Innovation - A Value-based System Design Approach* 2016, New York, London and Boca Raton CRC Press, Taylor & Francis. 284.
28. ISO, *ISO/IEC/IEEE 15288: Standard on Systems and software engineering — System life cycle processes*. 2015, ISO/IEC: Geneva, New York.
29. Kant, I., *Groundwork for the Metaphysics of Morals*, in *Practicle Philosophy*, M.J. Gregor and A.W. Wood, Editors. 1785/1999, Cambridge University Press: New York.
30. Stoltermann, E., *The Nature of Design Practice and Implications for Interaction Design Research.* International Journal of Design, 2008. **2**(1): p. 55-65.
31. Friedman, B. and D.G. Hendry. *The Envisioning Cards: A Toolkit for Catalyzing Humanistic and Technical Imaginations*. in *Computer Human Interaction (CHI)*. 2012. Austin, Texas, USA: ACM.
32. Bauer, C., & Spiekermann, S. (2011). Conceptualizing context for pervasive advertising. In Pervasive Advertising (pp. 159-183). Springer, London.
33. Dey, A. K. (1998, March). Context-aware computing: The CyberDesk project. In Proceedings of the AAAI 1998 Spring Symposium on Intelligent Environments (pp. 51-54).
34. Nissenbaum, H., *Privacy as Contextual Integrity.* Washington Law Review, 2004. **79**(1): p. 101-139.
35. Makena, K. (Feb 2019). "Google hired microworkers to train its controversial Project Maven AI". Internet: https://www.theverge.com/2019/2/4/18211155/google-microworkers-maven-ai-train-pentagon-pay-salary [Oct 2019].
36. Schaar, P. (2010). Privacy by design. Identity in the Information Society, 3(2), 267-274.
37. Sommerville, I., *Software Engineering*. Nine ed. 2011, International: Pearson.
38. Dybå, T., & Dingsøyr, T. (2008). Empirical studies of agile software development: A systematic review. Information and software technology, 50(9-10), 833-859.
39. Rierson, L. (2013). Developing safety-critical software: a practical guide for aviation software and DO-178C compliance. CRC Press.
40. Spiekermann, S. (2012). The Challenges of Privacy by Design. Communications of the ACM, 55(7).
41. Cooper, R.G., *Perspective: The Stage-Gate Ideal-to-Launch Process - Update, What's New, and NexGen Systems.* Journal of Product Innovation, 2008. **25**: p. 213-232.
42. Brown, T. (2008). Design thinking. Harvard business review, 86(6), 84.
43. Mill, J.S., *Utilitarianism*, in *Utilitarianism and Other Essays*, A. Ryan, Editor. 1863/1987, Penguin Books: London.
44. MacIntyre, A., *After Virtue: A Study in Moral Theory*. 2nd Edition ed. 1984, Notre Dame, Indiana: University of Notre Dame Press.
45. Winkler, T. and S. Spiekermann, *Twenty years of value sensitive design: a review of methodological practices in VSD projects.* Journal of Ethics in Information Technology, 2018.
46. Cutler, A., M. Pribic, and L. Humphrey, *Everyday Ethics for Artificial Intelligence - A practical guide for designers & developers*. 2018, IBM.
47. Microsoft, *2018 Corporate Social Responsibility report highlights*. 2018, Microsoft.
48. European Parliament and of the Council. 2016. " General Data Protection Regulation". Internet: https://eur-lex.europa.eu/eli/reg/2016/679/oj. [Oct 2019].
49. Solove, D.J., *A Taxonomy of Privacy.* University of Pennsylvania Law Review, 2006. **154**(3): p. 477-560.
50. Friedman, B., E. Felten, and L.I. Millett, *Informed Consent Online: A Conceptual Model and Design Principles*. 2000, University of Washington: Washington, USA.
51. Martin W., (22 September 2015). "Video statement Prof. Dr. Martin Winterkorn". Volkswagen. Retrieved via YouTube: https://www.youtube.com/watch?v=wMPX98_H0ak. [Oct 2019]
52. Howard, A., *Rapid Application Development: Rough and Dirty or Value for Money Engineering?* Communications of the ACM (CACM), 2002. **45**(10).
53. Lahlou, S., M. Langheinrich, and C. Röcker, *Privacy and trust issues with invisible computers.* Communications of the ACM, 2005. **48**(3): p. 59-60.
54. Bednar, K., S. Spiekermann, and M. Langheinrich, *Engineering Privacy by Design: Are engineers ready to live up to the challenge?* Information Society, 2019. **35**(3).
55. Zuboff, S., *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. 2019, New York: Hachette Book Group.
56. Craig M. Dalton. 2013. Sovereigns, Spooks, and Hackers: An Early History of Google Geo Services and Map Mashups. Cartographica: The International Journal for Geographic Information and Geovisualization 48, 4 (Dec. 2013), 261–274.
57. Ben Wagner, Till Winkler, and Marie-Theres Sekwenz. Comparing routing predictions: Travel time estimates and user accountability in navigation apps. In Workshop on Engineering Accountable Information Systems, European Conference on Information Systems - ECIS 2019, 2019.
58. Ahmed, P. and C. Shepherd, *Innovation Management*. 2012, New York: Financial Times/Prentice Hall.
59. Albright, R.E. and T.A. Kappel, *Roadmapping in the Corporation.* Research-Technology Management, 2003. **46**(2): p. 31-40.
60. Mueller, M. J., & Druin, A. (Eds.). (2012). Participatory Design. The third space in HCI (3rd Edi-tion ed.). Boca Raton, FL, USA: CRC Press.
61. MacIntyre, A. (1984). After Virtue: A Study in Moral Theory (2nd Edition ed.). Notre Dame, In-diana: University of Notre Dame Press.
62. Sen, A. (1993). Capability and Well-Being. In M. Nussbaum (Ed.), The Quality of Life. Oxford: Clarendon Press.
63. Nonaka, I., & Takeuchi, H. (2011). The Wise Leader. Harvard Business Review(May 2011), 58-67.
64. Detweiler, C., Pommeranz, A., vd Hoven, J., & Nissenbaum, H. (2011, September). Values in design-building bridges between RE, HCI and ethics. In IFIP Conference on Human-Computer Interaction (pp. 746-747). Springer, Berlin, Heidelberg.

65. Spiekermann, S., Winkler, T., & Bednar, K. (2019) A Telemedicine Case Study for the early phases of Value-based Engineering. In I. f. I. a. Society (Series Ed.), Working Pa-per Series/Institute for IS & Society: Vol. 1. Vienna: Vienna University of Economics and Business. URL: http://epub.wu.ac.at/7119/
66. van den Hoven, J. (2017). Ethics for the digital age: Where are the moral specs?. In Informatics in the Future (pp. 65-76). Springer, Cham.
67. Plattner, H., Meinel, C., & Leifer, L. (Eds.). (2010). Design thinking: understand–improve–apply. Springer Science & Business Media.
68. Sanders, E. B., & Stappers, P. J. (2008). Co-creation and the new landscape of design. CoDesign, 4(1), 5-18.
69. Mumford, E. (2000). A Socio-Technical Approach to Systems Design. Requirements Engi-neering, 5(2), 125-133.
70. Payne, S. (1951). The Art of Asking Questions. Princton: Princton University Press.
71. Winkler, T., & Spiekermann, S. (2019). Human Values as the Basis for Sustainable Information System Design. IEEE Technology and Society Magazine, 38(3), 34-43.
72. Winfield, A. F., Michael, K., Pitt, J., & Evers, V. (2019). Machine ethics: the design and governance of ethical AI and autonomous systems. Proceedings of the IEEE, 107(3), 509-517.
73. Dignum, V., Baldoni, M., Baroglio, C., Caon, M., Chatila, R., Dennis, L., ... & Micalizio, R. (2018, December). Ethics by Design: necessity or curse?. In Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society (pp. 60-66). ACM.
74. Force, J. T., & Initiative, T. (2013). Security and privacy controls for federal information systems and organizations. NIST Special Publication, 800(53), 8-13.
75. Spiekermann, S., J. Korunovska and M. Langheinrich (2018). "Inside the Organization: Why Privacy and Security Engineering Is a Challenge for Engineers." Proceedings of IEEE 107(3): 1-16.

Sarah Spiekermann received a masters' degree in economics from the European Business School ESCP-EAP (Paris- Berlin - Oxford) in 1997 and completed a Ph.D. in business informatics at Humboldt University Berlin, Germany in 2001.

She chairs the Institute for Information Systems and Society at Vienna University of Economics and Business (WU), Vienna, Austria. Before being tenured in Vienna in 2009, she was Assistant Professor at the Institute of Information Systems at Humboldt University Berlin (Germany), where she headed the Berlin Research Centre on Internet Economics (2003-2009). She was Adjunct Visiting Research Professor with the Heinz College of Public Policy and Management at Carnegie Mellon University (Pittsburgh, USA) (2006-2009). Her main research area is digital ethics and privacy.

Prof. Dr. Spiekermann is author of the books, “Digital Ethics” (Droemer, 2019), “Networks of Control” (Facultas, 2017) and “Ethical IT Innovation: A Value-based System Design Approach” (Taylor & Francis, 2016). Sind 2017 she is co-chair of IEEE's first standardization effort on ethical engineering (IEEE P7000). She has published in leading IS and CS Journals including the *IEEE Proceedings*, *Journal of Information Technology*, *IEEE Transactions on Software Engineering*, *Communications of the ACM, the European Journal of IS* (where she served as editor until 2013).

Till Wnkler. received a master in psychology at Leopold Franzens University in Innsbruck in 2016. Since then he is a Ph.D. student at the Institute for IS & Society at Vienna Universtiy of Economics and Business. Till Winkler has been part of the IEEE P7000 Working Group since 2017.

[1] The official link the IEEE P7000 is: https://sa-groups.ieee.org/7000/. The IEEE Working Group (WG) officially included 35 experts at the time of writing. These came with diverse backgrounds, mostly software- and system engineers, but also some with a deep expertise in philosophy. Participants were mostly from industry, a few academics, people from human-centric IT related think-tanks. Industry representatives varied throughout the years and included experts from the leading IT industry players to start-uppers (ranging from flying cars to telemedical or affective AI-based modeling) and independent consultants. The baseline for these expert's discussions was a P7000 draft that was written by the lead author of this article, which included an early version of value-based engineering. The learnings that were then collected from the P7000 WG and which this article is benefiting from could be gained from expert conversations in the group as well as more than 700 written impulses, critiques, and change requests shared in the WG and collected in three P7000 commenting periods in 2017, 2018 and 2019. We have integrated in our value-based approach that what seemed most valuable and in line with the existing academic approaches and insights. That said, we embrace terms and methodological steps here that the IEEE P7000 WG might not endorse and so there are divergences between the standard and some of the terms, recommendations and requirements presented here.

[2] The „design thinking“ schools at the Hasso Plattner Institute in Potsdam and in Stanford have been educating may innovation experts. For more information see: https://hpi.de/school-of-design-thinking.html or https://dschool.stanford.edu/

[3] Note that Material Value Ethics was created in the early 1920 and its reference is typically not machines, but rather people. So the terminology, which applicable to computer systems, has been developed with a view to social systems and has been transferred to computer systems in this research effort.