Ethics Inf Technol (2013) 15:173–181
DOI 10.1007/s10676-013-9326-1

ORIGINAL PAPER

Ethical requirements for reconfigurable sensor technology: a challenge for value sensitive design

Francien Dechesne · Martijn Warnier · Jeroen van den Hoven

Published online: 21 August 2013

Abstract Information technology is widely used to fulfill societal goals such as safety and security. These application areas put ever changing demands on the functionality of the technology. Designing technological appliances to be reconfigurable, thereby keeping them open to functionalities yet to be determined, will possibly allow the technology to fulfill these changing demands in an efficient way. In this paper we present a first exploration of potential societal and moral issues of reconfigurable sensors developed for application in the safety and security domain, in the context of a large scale R&D-project in the Netherlands. We discuss the subtle distinction between the relevant notions of reconfigurability, function creep, and unrestricted or unforeseen technological affordances. We argue that the feature of reconfigurability makes *context of use* the central issue in the assessment of the societal and moral impact of the technology. It follows that the design of good policies for new application contexts has to be central in a value sensitive design approach to reconfigurable technology.

Keywords Reconfigurability · Sensors · Security · Contextual integrity · Policy · Value sensitive design

The research presented in this paper is part of research project *Sensor Technology Applied in Reconfigurable systems for Sustainable security*: STARS.

F. Dechesne
Energy and Industry Section,
Department of Technology, Policy and Management,
TU Delft, Delft, The Netherlands

F. Dechesne (✉) · J. van den Hoven
Philosophy section, Department of Technology, Policy and Management, TU Delft, Delft, The Netherlands
e-mail: f.dechesne@tudelft.nl

J. van den Hoven
e-mail: m.j.vandenhoven@tudelft.nl

M. Warnier
Systems Engineering section, Department of Technology, Policy and Management, TU Delft, Delft, The Netherlands
e-mail: m.e.warnier@tudelft.nl

Introduction: reconfigurable sensors

Sensors are devices that measure physical properties and convert them into signals interpretable to an observer, for the purpose of recording or responding with action. Sensors such as cameras and motion detectors have proven to be practical sources of information that can be used in the effort to provide safety and security for a society in general, and to help resolve crisis situations. Sensors are connected in networks, thereby facilitating collecting the information, analyzing it, and making it accessible to human decision makers.

The application areas of safety and security have given a strong impulse to the development of sensor technology, because it provides efficient ways of monitoring various kinds of situations, both involving technological and human behavior. This impulse has been clearly visible, for example, in the post 9/11 aviation sector [with mixed results: Johnson (2006), King (2011)]. Applications to safety and security also motivated a large scale, 4.5 year research project in The Netherlands: Sensor Technology Applied in Reconfigurable systems for Sustainable security (STARS 2010). The STARS project involves both academic and private research partners. The goal of the project is the development of "necessary knowledge and technology to be able to build reconfigurable sensors and sensor networks." By making sensors reconfigurable, the project aims to deliver a continuous and affordable infrastructure

for societal security. The reconfigurability contributes to the affordability by keeping other application areas as open as possible: this should reduce the need to develop new technology for every new desired functionality. Reconfigurable parts of sensor networks that will be looked at are antennas, receivers, transmitters, on-chip and off-chip communication. As an example, reconfiguration of the sensors should make it possible to transform a sensor network installed in a harbor for security purposes, e.g. to prevent theft or sabotage, into an information system for rescue workers during a fire in the same harbor.

In this paper we intend to show how the reconfigurability of sensor technology, as envisaged in STARS, adds an extra challenge for efforts towards including moral and societal considerations in the technology design. The extra challenge of reconfigurable technology arises from pushing the specification of the intended functionality and intended use forward, outside of the technology design phase. We present a first conceptual exploration of the societal and moral implications of reconfigurable sensor technology such as the technology developed within the STARS-project. We present the questions we think will be the relevant ones, both for the conceptual, and for the empirical and technical aspects of the design process.

Reconfigurable sensor technology for the security domain

Among the characteristic aspects of the security domain are the diversity of threats, and the absence of warning time. The opponent is unpredictable: he cannot be expected to comply with any rules, and will be creative. Hence, maintaining security means to be able to anticipate and respond adequately to new situations. The societal problem is that it takes too long, and that it is too expensive, to invest over and over again in the development of new systems to protect against changing threats. Successful security technologies should therefore satisfy a number of requirements: to be reliable and affordable, sustainable and effective, multi-domain and multi-service. In the STARS-project, reconfigurable sensors are developed to have these characteristics. Their design is intended to allow for flexible application, where the possible functionalities of the system should be relatively easy and quickly to adapt.

In the initial architecture definition of the STARS-sensors, there are three different types of base stations, to which sensor modules of different types (e.g. radio frequency, infrared, sonar) can be attached. For flexible functionality, the base stations can be (re)positioned strategically, the sensor modules can be replaced by other types, and the settings of the modules can be adapted (e.g. one can switch to other frequencies).

With this specific setting in mind, we distinguish three reconfiguration levels: reconfiguration by tuning *parameters* (almost instantaneous, possibly remote), reconfiguration of the *arrangement* of sensors at a certain sensor node (which may require those sensors to be offline for a short time), and substantial structural reconfiguration, where components are removed or added (which may require the sensor node to be relocated and out of order for a longer period of time). In STARS, all three types of reconfiguration are envisaged, with different levels of functional flexibility associated to them. For example, instantaneous reconfiguration should be available to optimize for *foreseen* situations and the corresponding tasks. In future scenarios that are yet unforeseen, the reconfiguration may have to be more structural: Functionality that is radically different from the one envisaged in the current configuration, could also require more radical reconfiguration. (Note however that this is not necessarily the case: we will come back to the relationship between configuration and functionality in "Reconfigurable technology" section.)

With the flexibility and adaptability of the functionality as motivation, the feature of reconfigurability is leading in the design and development of the architecture and technologies in the STARS-project. The use cases that are initially defined within project, primarily restrict the envisaged users to police, fire brigade, security- and information services. However, it is expected that the technology, if successful, will cover a broader application area by a broader range of users. During the project, system concepts and application potential are to be defined and explored.

Restricted perspective on reconfigurability

To avoid misunderstanding about the scope of this paper, we should point out that we take a restricted perspective on reconfigurable sensor technology, one that stays close to the reconfigurability expected in STARS. It is worthwhile to make some remarks on the relationship between this restricted account, and the topics of ambient intelligence, and pervasive/ubiquitous computing. In short, we could say the latter topics are essentially about the presence of computing power in (interconnected) devices and how this can be used for a broad range of applications: they are about 'smart' objects (mostly equipped with sensors), which are reconfigurable by virtue of their computing power. Such systems do share with STARS a broad (and potentially flexible) range of functionality. An ambient intelligence/pervasive computing system as a whole may be considered to be reconfigurable. However, it is reconfigurable in a more general sense than the sensor technology in STARS, where the reconfigurability lies in the sensors rather than in (adding) computing power.

To illustrate this, we mention some work from the literature on ubiquitous computing and ambient intelligence. For example, Bellotti and Sellen (1993) describes a case study ("the RAVE network") which features a sensor network where the users are at the same time objects of observation—whereas the users in STARS are enforcement agencies who observe an external environment. It uses a framework [of Gaver et al. (1992)] focusing on control and feedback: control encompasses "empowering people to stipulate what information they project, and who can get hold of it", and feedback "informing people when and what information about them is being captured and to whom the information is being made available." These are general principles that can be guiding for ensuring a reasonable degree of privacy in surveillance systems. In particular the feedback aspect could be useful for STARS sensors. The fact that the issue of control will be hard or impossible for the objects of observation, points to a fundamental problem with STARS sensors (and surveillance for security in general). The ubiquitous computing platform in Ortmann et al. (2007) also differs from STARS in the fact that the sensors are intended for a different type of users: users who both observe and are being observed.

We will come back to our restricted perspective on reconfigurability in "Reconfigurable technology" section.

Anticipating societal and moral impact of reconfigurable sensor technology

The development of reconfigurable sensor technology is aimed at impacting the societal goals of safety and security. But the overall societal impact is not just determined by the technical features and their intended functionality. We approach this technology as a socio-technical system, which means that we take the embedding of the technology in social and societal structures to be of essential importance to its effect: What data will be gathered and by whom? Who will handle the data? How will the data be used? Who determines the priority of functionalities when the system is intended to serve different goals? We believe the aspect of reconfigurability makes these questions both more complex, and into the crucial part of the societal success of the technology.

The open functionality of reconfigurable technology and its intended wide applicability within society ['logical malleability' in the terminology of Jim Moor's seminal 1985 article Moor (1992)], require that societal and moral values are considered in the application phase. Ideally this is anticipated already in the design phase. This is the main principle behind the programme of *value sensitive design* (VSD), a "theoretically grounded approach to the design of technology that accounts for human values in a principled and comprehensive manner throughout the design process" (Friedman et al. 2006). VSD distinguishes three types of activities: conceptual, empirical and technical, which are integrative and iterative.

This paper aims to show how the reconfigurability of sensor technology, as envisaged in STARS, adds an extra challenge to VSD. The flexibility of reconfigurable technology necessitates new tools, for instance to keep track of different and evolving contexts of use. In particular, the design of good usage policies—including: what are boundary conditions for the use of the technology in a certain configuration in a particular context?—becomes crucial.

The paper is structured as follows. In the next section, we describe a use case from the STARS project to illustrate the reconfigurable sensor technology and a possible context of use for which it is being developed. In "Reconfigurable technology" section, we reflect from a more theoretical perspective on the feature and concept of reconfigurability. In "Ethical impact of reconfigurability?" section, we connect the issues that come with reconfigurability to VSD. In "Applicability of the framework of contextual integrity" section, we argue that *contextual integrity* is a useful notion for reconfigurable technology, indicating that the specification of contexts of use will add importance to policy design. We end the paper with a discussion of our findings, some concluding remarks and issues for further work.

Use case: safety and security domain

The intended application of the reconfigurable sensors and sensor networks in STARS is the safety and security domain. A use case for the sensor networks is the situation at a large port area (for example, the port of Rotterdam or Shanghai). Radar systems are used in large ports to monitor the movement of ships. Ship sizes can also be determined by these systems. Such radar systems consist of a number of radar devices, which send their collected data to a central control center. Here the data is processed to provide a full overview of the whole area. Other sensor data, for example from camera surveillance systems [closed circuit television (CCTV)] or motion detectors (around security gates) are also sent here, providing even more information in case of an incident.

Numerous issues around safety and security can arise in a port environment, including fire hazards, drug or people trafficking, terrorism or transport of hazardous chemicals. During an incident all sensor data can be combined to coordinate emergency services. Reconfigurable sensors could be especially useful in such environments, since they are intended to be usable for different tasks as the need arises, whereas previously multiple sensor systems would have been required. Consider, for example, the case where

a small plane crashes into the port area. The police might be worried that this is part of an organized terrorist attack, in which case (part of) the radar system can be reconfigured to look for other (low flying) planes. Information provided by the reconfigured radar system can be crucial for the police (and other services) to gain control of the situation.

The reconfigurability of the sensors provides more flexible functionality, but it also introduces a number of potential problems. First of all, by reconfiguring the radar system, the 'normal' radar view of the ships in the harbor is compromised: the spatial resolution will go down, making it harder to distinguish different ship sizes. Part of the harbor may not be visible at all. This might be acceptable in a crisis situation, but it does lead to another issue: Who decides if the radar system may be reconfigured, and under which circumstances? Is the fire brigade in charge or the police? Or perhaps the port authorities or the government? Clear policies need to be defined for this, policies that can become more complex as the sensor systems' reconfigurable functionality increases. Even if the aim is to make the technology almost instantaneously reconfigurable, it is still likely that there will be some processing time needed for each reconfiguration. This can be crucial in crisis situations: during reconfiguration sensors cannot be used, leaving the control center in essence blind to the current situation. This may be acceptable if reconfiguration time is in the range of fractions of seconds, but longer delays may compromise the usability of the technology. So, only certain types of reconfiguration are realistic for certain situations.

The potential problems with reconfigurability mentioned above, stem from the same core problem: reconfigurable systems may provide multiple functionality and be flexible in extending functionality, but they cannot necessarily provide the functionalities concurrently. One can either search for ships or for low flying planes, not both (at the same time). An important part of the activity of VSD (Friedman et al. 2006, Section 6) consists of identifying the values associated with the benefits and harms of the technology, analyzing them, and identifying potential value conflicts. Reconfigurability of the technology significantly adds complexity to this already difficult task of identifying, balancing and prioritizing values, especially if different values are supported by different functionalities. Who gets to decide which value should be given priority in such situations?

A policy is a plan of action or procedure put in place by a governing body to determine actions and decisions with the aim to achieve a certain goal. A simple example of a policy for STARS-technology in the port case, could be the identification for three general situations in the context of which the sensor network will be used, for example Normal Operation of the Port (code Green), Hazard or Accident (code Orange) and Malicious Threat or Attack (code Red). The policy then prescribes for each of these situations how the (initial) configuration of the sensors should be, and who will be in control and responsible for the operation of the sensor network in this situation (e.g. the Fire Brigade for code Orange, and the counter-terrorism coordinator of the Ministry of Interior Affairs for code Red). This implies policies on different levels: policies concerning control over the sensors on the lower level, and higher level policies on who is responsible for declaring the general state (Green, Orange or Red).

Although policy design may not in itself be part of technology development, the VSD perspective requires that in the design of the technological artifact attention is paid to the aspect of governance (e.g. to fulfill values such as trust). With each policy comes an information flow of a certain granularity and with a certain focus. Such aspects of the policies will most probably and efficiently be implemented into the technology. We also believe that with the reconfigurability in STARS, the flexible functionality asks for the design of default policies, at least for foreseen usage, for example by defining default configurations for default situations. This should be anticipated when designing the technology, because controlling and evaluating mechanisms may be hard to implement as add-ons.

The framework of VSD suggests to start in practice from either a value, a technology or a context of use (Friedman et al. 2006). Whereas reconfigurable technology deliberately aims to remain as flexible as possible to serve different goals (values), it becomes central to take a context of use as starting point. Indeed, the questions raised above are practically unanswerable without delineating a specific context of use first. It is important to realize that the ethical evaluation of the technology highly depends on the context of use, making the specification of the context a *sine qua non* for the integration of societal and ethical aspects into the design and application of the technology.

Reconfigurable technology

The VSD approach distinguishes *conceptual activities* as one of the three types of activities of the approach. When addressing the ethical and societal impact of reconfigurable sensor technology, it is useful to clarify the notion of 'reconfigurable technology.' In particular, we deem it to be useful to analyze the relationship between (re)configuration and (flexible) functionality and usability of the technology. We will try to clarify the relationship between reconfigurability on the one hand, and concepts referring to the use of technology on the other, such as *function creep* and the flexibility of technological *affordances*.

Literally, 'reconfiguration' means: modification of the configuration, i.e. rearrangement of the parts (of a system).

For example: the modification of a radar system so that it can scan for low flying planes instead of boats. Implicitly, at least within the STARS-project, it is taken that new configurations will enable new functionalities and usages, in particular: functionalities that may not yet have been specified when the technology was developed. Hence, reconfigurability should serve to provide a flexibility in functionality beyond the design phase. Because the term 'functionality' often bears the connotation of being the particular use *for which something is designed*, it helps to also bring in Gibson's terminology of *affordance* (Gibson 1986) in order to also talk about more general usage. Affordances of a technology can be defined as the action possibilities latent in the technology, and need not be designed-in intentionally. This is demonstrated in the *dual use*-problem: technologies designed with a peaceful functionality, such nuclear radiation technology for cancer treatment, or aviation technology for the transportation of people, also bring the affordance of harmful usages.

We would like to point out that configuration on the one hand, and functionality and affordance on the other, by no means have a one-to-one relationship. A piece of technology can have different functionalities (or affordances) without being reconfigurable. A simple stone can be a missile, but also a "paper weight, a bookend, a hammer, or a pendulum bob" (Gibson 1986, p. 134). Also, a car can be both a means of transportation and a deadly weapon if intentionally used to drive into a group of people. Conversely, not every rearrangement of parts will necessarily lead to new affordances of the technology. So, while the STARS project focuses on making the sensors reconfigurable in order to achieve flexible functionality, part of the research should also address the question to which extent this ultimate goal is achieved in the developed technology.

We described "reconfiguration" very generally as a modification of the arrangement of parts, but this does not draw clear borders as to what counts as reconfiguration and what type of modification goes beyond reconfiguration. To which extent can we speak of reconfiguration when we don't just rearrange *existing* parts but (also) add *new* parts, or even technologies? For example, it is current practice to extend the affordances of sensor systems by processing the signals using computers. Think for example of the enhancement of CCTV systems with software that processes faces and compares these to a database with known subjects (Zhao et al. 2003) in order to identify them. In a sense this extension could be described as a reconfiguration of the CCTV system, since the original configuration of the system is changed for a specific purpose. In this paper however, we take it that not every alteration or extension of a technological system necessarily counts as a *reconfiguration*. In particular we will not include situations where new technologies are brought into the system, such as the face recognition layer to the camera observation (we would call this *synthesizing* technologies rather than *reconfiguring* the sensor system).

We can see the STARS-project as a specific case of a development process for reconfigurable technology. In this concrete case, what kind of reconfigurability can we expect? The ultimate goal of the project is to develop sensors and sensor networks with as much (potential) functionality as possible. The project proposes to achieve this by making the hardware reconfigurable, which involves mainly analogous front-ends (infrared, radar, etc.) and digital signal processing. We think the resulting range of possible reconfigurations will be limited to the three types of reconfiguration we have identified in the introduction: adaptation of parameters, switching modules and more structural reconfiguration of the base stations.

Although this is a rather limited range of reconfiguration, we believe it provides an interesting starting point to our reflection on reconfigurability and the applicability of VSD. Methodological questions are already raised by making parts of the architecture reconfigurable, such as those concerning testing procedures, software-hardware partitioning and composability [as pointed out for reconfigurability in the context of software architecture in Guo (2006)].

On a higher order level, one could state that STARS aims to create the affordance to address future, yet unknown, applications by making the technology reconfigurable. In our involvement in the STARS-project, we aimed to identify specific ethical challenges related to the reconfigurability of technology, although this also touched upon more general issues of multiple and flexible functionality. The goal of this endeavor, in line with the VSD approach, is to create awareness and anticipate these challenges in the research and development phase of the technology.

Ethical impact of reconfigurability?

When looking for ethical challenges raised by the feature of reconfigurability, it is natural to turn to ethical theories for what seems the ultimate reconfigurable technology: the 'universal machine', i.e. the computer. In his seminal paper "What is Computer Ethics?" (Moor 1992), James Moor refers to the *logical malleability* of computers as the essence of the revolutionary character of computer technology, from which the need for a separate attention for computer ethics follows:

> "The essence of the Computer Revolution is found in the nature of a computer itself. What is revolutionary about computers is logical malleability. Computers are logically malleable in that they can be shaped and

> molded to do any activity that can be characterized in terms of inputs, outputs, and connecting logical operations. […] This is all I need to support my argument for the practical importance of computer ethics. In brief, the argument is as follows The revolutionary feature of computers is their logical malleability. Logical malleability assures the enormous application of computer technology. This will bring about the Computer Revolution. During the Computer Revolution many of our human activities and social institutions will be transformed. These transformations will leave us with policy and conceptual vacuums about how to use computer technology. Such policy and conceptual vacuums are the marks of basic problems within computer ethics. Therefore, computer ethics is a field of substantial practical importance." (Moor 1992)

Here the logical malleability of computers is taken as the central cause of several effects computers will have on society, and from these effects, the need for computer ethics follows. We explore what ethical issues follow from the aspect of reconfigurability in itself (hence, not just from the instantiated effects) in reconfigurable technology. Does reconfigurable technology ask for different types of functional and non-functional requirements? Do we need to specify meta-requirements to capture requirements on the level of the reconfiguration process?

An important aspect of reconfigurability is that it challenges the type of stable, knowable, unambiguous function ascriptions to artifacts and systems. It raises epistemological issues related to agency. The STARS-project, one could say, takes it as a goal to defer the specification of functionalities for the technology past the design phase, even past the implementation phase, to remain flexible during the use phase. In that sense, the central feature of reconfigurability may ask for an extension of existing theories of technical functions (Houkes and Vermaas 2010). An implication of this observation, is that the developers of the technology can only to a lesser extent be expected to anticipate values and social consequences of the use of the technology. Because of the reduced knowability of the usage of the technology, agency with respect to social and moral consequences shifts from those involved in the development to those involved in the actual use (users, or policy makers). This puts limits on a VSD approach to the actual technology development, and shifts importance to value sensitive policy design. On a meta-level however, one could say that the developers should know this, hence bear responsibility for technology design that enables good policy design for as wide a range of applications as possible. Hence, guidelines for the use of reconfigurable technology can (and must) be given by its designers. These can include meta-rules that state how to deploy the system for a specific context, such as the example of the large port area discussed above, and make the reconfigurable usage of the system explicit in policies.

The epistemological issue connected to the open functionality clearly bears on the principle of informed consent. A prerequisite of that principle is a knowable impression of what the system will do under which circumstances. One can argue that this prerequisite is hard to fulfill for many of today's (socio-technical) systems, as they are developed for a certain goal, but once in place, easily used for or combined with other functionalities. This is called function creep; a well known example is the use of cameras that are put in place to implement a road pricing system, also for the detection of stolen cars, or tax evaders. This issue is even more prominent if the system is intended to be reconfigurable to changing circumstances, or even designed to fit yet unthought of functionalities and affordances. This could be called: "function-creep-by-design", open-ended design intended for open-ended use. At what level of abstraction can the system's behavior be specified for people subject to it, and is that enough of a basis for them to be able to consent or as a basis to justifiably assume their consent? A clear specification of the context of use becomes crucial for the users to be able to truly decide on consent. In the example of the port area: if the goal and potential use of the reconfigurable sensor system are not know and the main actors (police, fire brigade, counter-terrorism coordinator) are not identified, it becomes impossible to write policies on how the reconfigurable system should be used.

The specification of the behavior of the system requires a sophisticated and complex balancing of the different values the different functionalities of the technology serve. Combining technology for flexible and multiple functionality into one sensor, adds the restriction that only one functionality at a time can be actually used: concurrent use of different functionalities may not be possible. This means that more crucially than usual, priorities of the different functions must be assigned. This adds an extra dimension to the design process, namely the necessity of designing policies to specify priorities. But these policies should also be flexible to deal with the flexible functionality of the technology. Thus, in the port example, it is important to specify who (fire brigade, counter-terrorism coordinator) should have control about the reconfigurable sensors in which situation (chemical fire, terrorist attack). But the responsible actors should be able to decide for themselves how the sensor are to be configured and used; the policy should not be overly restrictive.

Reconfigurable technology comes with two sources of complexity: the technical complexity raised by the reconfigurability (which is deterministic), and the complexity associated with the fact that the application of the technology is deliberately left open (which is even non-monotonic). The

latter will be the biggest challenge to address. Indeed, the observations above show that the reconfigurability leads to an increased range of choices that need to be made to put the technology to use. These choices address not only practical aspects, but more essentially higher order choices: who will be in control of such (practical) choices? Who will bear responsibility for the different functionalities, or for the system as a whole? This indicates that the development of policies around reconfigurable systems will bring in new complexities. Such complexity may compromise the expected efficiency of reconfigurability.

Applicability of the framework of contextual integrity

The reconfigurable sensor networks primarily envisaged in STARS may be intended as *closed* systems, in the sense that the network will only be open to explicitly authorized users, and this group of users will be more or less stable and uniform (in particular: order preserving authorities, such as fire fighters, police, port authorities). The problem with the reconfigurability is that the contexts in which the technology may be used is deliberately left as open as possible in the design of the technology.

While the initial use case for the reconfigurable sensor networks is not primarily related to the observation of persons and their behavior, we deem it useful to look at the ethical issues related to sensor networks like camera surveillance and RFID access control systems. There is extensive literature discussing how sensor networks for observation of individuals and their environment bring up issues concerning privacy and the protection of personal data, such as Chan and Perrig (2003), Shi and Perrig (2004), and the legally oriented account in Solove (2008). Also, we expect that the technology may in the future be applied in privacy sensitive ways. This not just because the functionality is left open to future use and might include observation of individuals, but also because with increasing data collection surrounding all transactions in society, and linking of databases, objects and transaction traces can be more and more easily linked, also to people. This means that object data may turn into personal data a posteriori. But besides that, we argue that central notions from the discussion of privacy may be helpful in the analysis of reconfigurability, in particular the notion of *context*.

Conceptual solution: reconfigurability in context

Reconfigurability puts the context of use and control of information—captured in notions such as 'spheres of justice' or 'spheres of access' (Hoven 1999; Nagenborg 2009) and 'contextual integrity', as used by Ackerman et al. (2001), Nissenbaum (2010)—even more crucially at the heart of the challenge put forward by privacy. For example, Nissenbaum understands privacy in terms of context-relative information norms, and distinguishes norms of appropriateness, and norms of distribution. She defines contexts as "structured social settings, characterized by canonical activities, roles, relationships, power structures, norms (or rules), and internal values (goals, ends, purposes)" (Nissenbaum 2010, pp. 132–134). Most relevant to the framework of Contextual Integrity are the roles, activities, norms and values. For reconfigurable systems there may be different roles, activities, norms and values that need to be combined in the design of one system, and its usage policies. How to deal with the composition of these different contexts for one system is a particular challenge.

Reconfigurability involves applicability of one system with flexible functionality in possibly distinct contexts. In the case of reconfigurable sensor networks, the challenge will be to formulate requirements that are both general and specific enough to cover each possible use. For example, how to balance privacy issues if the sensor system monitors individuals only in very few of its configurations? And how to go about changes in this configuration?

Practical solution: context dependent policies (values in context)

Nissenbaum's framework for Contextual Integrity provides explanation, evaluation and prescription, and thereby contributes to the design process. As Nissenbaum recognizes, it does not yet "support substantive descriptions for general families of technologies", and "the most fruitful assessments take place within particular contexts" (Nissenbaum 2010, p. 190). In the case of reconfigurable systems, the particular context may be underspecified, or only one of a vast number of possible contexts. Therefore, a specific challenge for VSD of reconfigurable technology, such as sensor networks, requires an analysis of the composition and interaction of different contexts, and its translation into policies.

We can conclude that in the case of the development of reconfigurable technology, or more accurately: technology that provides "function creep by design", the applicability of VSD is limited, and it may be more fruitful to focus on "values in context of use". This corresponds to a shift from the "technical" to the "social" component of socio-technical systems: technology developed to provide open affordances will not constrain the value choices, so this is left to the actors in the social context.

Discussion

Reconfigurability of sensors in networks seems to be an attractive answer to the increasing and invariably changing

demands in the security and crisis management domain, both in terms of economy and of effectiveness. The central aim behind the reconfigurability of the technology developed in STARS is to keep the use of the technology open to future functionalities, uses that are not explicitly envisaged yet in the design phase of the technology. In other words, the technology is designed to provide the affordance to address future, yet unknown, applications by making the technology reconfigurable. *Function creep* is replaced by the explicit goal of *function shift* towards yet undefined functionalities. Configurations could change overnight towards new functionality—but how do people subject to it or using it get to know this? Reconfigurability thereby implies that there is uncertainty about what the current normative framework is (which is an epistemic problem). This means the VSD approach has to start from a definition of a context of use.

Although at first sight, one could say that the sensor networks of STARS are intended to be closed systems, in the sense that the amount of user parties is limited and coordinated, reconfigurability gives the sensor networks open traits of a slightly different kind. The openness towards its functionality makes that systems' role based access models should also be reconfigured with the system. This contributes to the non-technological complexity of reconfigurable technology, an aspect which is not to be overlooked.

We expect the non-technological complexity of reconfigurable sensor technology to surface in particular around the ethical issue of privacy. Even if the STARS-sensors are not primarily intended for monitoring persons, privacy will inevitably become relevant in at least part of the usages of the STARS-technology over the coming years. One has to be aware that what counts as "personal data" is being stretched by connecting data from various sources, data gathered about objects are easily linked to (data about) people, and thereby transitively become personal data after all. Furthermore, the fact that privacy is recognized a human right in the UN Declaration of Human Rights, makes it always a juridical constraint. The European Union expects from companies and research consortia to take their own responsibility (*responsible innovation*): they should be able to justify how they dealt with constraint/secured values. For the case of reconfigurable sensor technology, with its *function-creep-by-design*, it follows that privacy issues should be accounted for, regardless whether the current, or currently intended, use deals with personal data.

Conclusion and further work

In this paper, we have presented an initial, mostly conceptual reflection on challenges that reconfigurable technology raises for VSD. Functionality and even goals of the technology are deliberately left open in the design phase of the technology, so the assessment of the ethical and societal impact of the technology heavily depends on the definition of contexts of use, and the importance of policy design for the use of the technology in each such contexts increases.

In the coming years, with the progress of the STARS-project a more thorough analysis of the concept of reconfigurability will be possible. It will be interesting to see how reconfigurability can be analyzed from the perspective of the literature on function ascriptions and requirements engineering. Is (physical) reconfiguration essentially different from re-conception of the possible use of a piece of technology? We believe that a proper analysis and definition of context and spheres will be crucial in the VSD of such technology: it is essential both for understanding its potential effects and, in practice, for the formulation of usage policies.

Acknowledgments We are grateful to the audiences at the 17th International Conference of the Society for Philosophy and Technology (SPT), May 2011 in Denton (Texas, USA), and the Workshop on Values in Design, in Lisbon (Portugal), September 2011, for the discussions leading to this paper. Furthermore, we thank the anonymous referees for their constructive comments on earlier versions of this paper, and for the pointers to related work.

References

Ackerman, M., Darrell, T., Weitzner, D. (2001). Privacy in context. *Human-Computer Interaction 16*, 167–176.

Bellotti, V., & Sellen, A. (1993). Design for privacy in ubiquitous computing environments. In: *Proceedings of the third European conference on computer-supported cooperative work* (pp. 77–92). Kluwer: Kluwer Academic Publishers.

Chan, H., & Perrig, A. (2003). Security and privacy in sensor networks. *IEEE Computer 36*(10), 103–105.

Friedman, B., Kahn, P. Jr, & Borning, A. (2006). Value sensitive design and information systems. In P. Zhang, & D. Galletta (Eds.), *Human-computer interaction in management information systems: Foundations* (pp. 348–372). NY: M.E. Sharpe, Inc.

Gaver, B., Moran, T., MacLean, A., Lövstrand, L., Dourish, P., Carter, K., & Buxton, B. (1992). Realising a video environment: EuroPARC's RAVE System. In *Proceedings of the ACM conference on human factors in computing systems, CHI 92* (pp. 27–35). New york: ACM Press.

Gibson, J. J. (1986). The theory of affordances, In *The Ecological Approach to Visual Perception* (Chap 8, pp. 127–143). Hillsdale, New Jersey: Lawrence Erlbaum Associates, Inc., Publishers. (Originally published 1979).

Guo, Y., (2006). Mapping applications to a coarse-grained reconfigurable architecture. PhD thesis, University of Twente, Enschede.

Houkes, W., & Vermaas, P. E. (2010). *Technical functions: On the use and design of artefacts (philosophy of engineering and technology)*. Berlin: Springer.

Hoven, M. J. (1999). Privacy or informational injustice?. In L. Pourcia (Ed.), *Ethics and information in the twenty-first century* (pp. 140–150). West Lafayette, Indiana: Purdue University Press.

Johnson, R. C. (11 Sept. 2006). Post-9/11, technology keeps us a step ahead, EE Times News & Analysis. http://www.eetimes.com/electronics-news/4064803/Post-9-11-technology-keeps-us-a-step-ahead. Accessed October 12, 2012.

King, R. S. (Sept. 2011). How 5 security technologies fared after 9/11—developed, deployed, and sometimes deep sixed. IEEE Spectrum: Biomedical/Devices. http://spectrum.ieee.org/biomedical/devices/how-5-security-technologies-fared-after-911. Accessed October 12, 2012.

Moor, J. H., (1992). What is computer ethics?, Southern Connecticut State University, New Haven, CT, USA, pp. 1–11. Reprint of Moore, J. (1985). What is computer ethics?. Metaphilosophy, 16(4):266–275.

Nagenborg, M. (2009). Designing spheres of informational justice. *Ethics and Information Technology 11*, 175–179

Nissenbaum, H. (2010). Privacy in Context. Stanford, CA: Stanford University Press.

Ortmann, S., Langendörfer, P., & Maaser, M. (2007). A self-configuring privacy management architecture for pervasive systems. In: *Proceedings of the 5th ACM international workshop on mobility management and wireless access*. ACM, New York, NY, USA.

Shi, E., & Perrig, A. (2004). Designing secure sensor networks. *Wireless Communication Magazine 11*(6), 38–43.

Solove, D. J. (2008). Understanding privacy. Cambridge, MA: Harvard University Press.

STARS-project. (2010). STARS project information, available at the STARS-Project website: http://starsproject.nl/.

Zhao, W., Chellappa, R., Phillips, P., & Rosenfeld, A. (2003). Face recognition: A literature survey. *ACM Computing Surveys (CSUR) 35*(4), 399–458.