Health Care Anal (2015) 23:148–164
DOI 10.1007/s10728-013-0262-3

ORIGINAL ARTICLE

Privacy by Design in Personal Health Monitoring

Anders Nordgren

Published online: 27 August 2013

Abstract The concept of privacy by design is becoming increasingly popular among regulators of information and communications technologies. This paper aims at analysing and discussing the ethical implications of this concept for personal health monitoring. I assume a privacy theory of restricted access and limited control. On the basis of this theory, I suggest a version of the concept of privacy by design that constitutes a middle road between what I call broad privacy by design and narrow privacy by design. The key feature of this approach is that it attempts to balance automated privacy protection and autonomously chosen privacy protection in a way that is context-sensitive. In personal health monitoring, this approach implies that in some contexts like medication assistance and monitoring of specific health parameters one single automatic option is legitimate, while in some other contexts, for example monitoring in which relatives are receivers of health-relevant information rather than health care professionals, a multi-choice approach stressing autonomy is warranted.

Keywords Ethics · Health monitoring · Privacy · Privacy by design · Telecare

Introduction

The concept of privacy by design is becoming increasingly popular among regulators of information and communications technologies. For example, it is about to find its way into EU regulations in terms of “data protection by design”. This is how the idea is expressed in the recent proposal for a “General Data

A. Nordgren (✉)
Centre for Applied Ethics, Linköping University, 581 83 Linköping, Sweden
e-mail: anders.nordgren@liu.se

Protection Regulation” from the European Commission to the European Parliament and the Council:

> Article 23: Data protection by design and by default
> 2: The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals [4].

This paper aims at analysing and discussing the ethical implications of the concept of privacy by design for information and communications technologies used in personal health monitoring. Personal health monitoring is a rapidly developing field. Examples of technologies are electronic medication assistance, sensors for monitoring heart failure, sensors for fall detection, night vision cameras, and mobile safety alarms. This type of monitoring is expected to improve quality of life by giving patients opportunity to stay longer at home and to reduce health care costs for an ageing population by reducing the number of visits to hospitals and nursing homes [5, 9, 10]. The analysis pinpoints the potential as well as the limitations of the concept of privacy by design in this context.

My analysis takes as a point of departure the understanding of the concept of privacy be design suggested by Ann Cavoukian, Information and privacy commissioner of Ontario, Canada. One reason for this choice is that Cavoukian was the first to develop this concept in detail, another that Cavoukian recently addressed the implications of this concept for personal health monitoring ([1]; note that below I refer to “Cavoukian” despite the fact that she in this article has several co-authors).

Privacy by Design

This is how Cavoukian explains the concept of privacy by design in terms of seven basic principles:

1. Proactive, not reactive; preventative, not remedial
2. Privacy as the default
3. Privacy embedded into design
4. Functionality—positive-sum, not zero-sum
5. End-to-end lifecycle protection
6. Visibility and transparency
7. Respect for users’ privacy [1].

The first principle emphasizes that respect for privacy should be included before the technology is developed, rather than after it is developed. The second means that data will be protected automatically. The third principle says that privacy should be built into the technology, not be something extra that is added afterwards. The fourth principle is that we need not choose between privacy and security. It is possible to have both. The fifth stresses that data should be protected in all data handling from beginning to end. The sixth principle states that data protection should be open to independent scrutiny. The last principle emphasizes that the focus in technology development should be on the individual. It should be user-centred [1].

It is not quite clear what Cavoukian's concept really means. Most of the principles she uses to explain privacy by design include privacy by design in the explanation. It is clear, however, that for Cavoukian privacy by design is a matter of "embedding privacy into the design specifications of technologies". Moreover, Cavoukian talks about "end-to-end lifecycle protection" and explains that this means that privacy by design should be included in all data handling from "cradle to grave", i.e., from before the first piece of data is collected throughout the whole process of management of data—including "properly executed log data files"—until the data is finally destroyed [1].

A key aspect of privacy by design seems to be data minimization. Cavoukian refers to OECD's "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", which include eight principles: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability [11]. With these principles in mind, Cavoukian declares:

> We will explore how Privacy by Design may be used to integrate these principles—and data minimization in particular—into specific remote home health care technologies [1].

The European Commission's version of privacy by design in terms of "data protection by design", mentioned above, also stresses the idea of data minimization: "only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes" [4].

Is this concept of privacy by design—as proposed by Cavoukian and the European Commission (in terms of data protection by design)—ethically acceptable? Below I will discuss various aspects of this concept.

The Concept of Privacy

The concept of privacy can be understood in many different ways. It follows that the concept of privacy by design, which presupposes this concept, can also be understood in various ways. This makes it important to analyse Cavoukian's understanding of privacy, relate it to other views and take a stand on its acceptability.

We talk about privacy in many different contexts, for example, information, activities, decisions, thoughts, body, communication and space (see, for example, [15, 17]). Cavoukian focuses on "information privacy". This is how she defines this concept:

> Information privacy is an individual's ability to exercise control over the collection, use, disclosure and retention of his or her personal information, including personal health information [1].

It appears that Cavoukian proposes a control theory of privacy. This is one of four types of privacy theory distinguished by Tavani [18].

The first theory focuses on the non-intrusion, i.e., to be left alone. Tavani argues that this view confuses privacy with liberty. These two concepts are closely related but they can also be distinguished. It is liberty that allows an individual to hold politically unpopular ideas, but it is privacy that allows him to disclose these ideas to certain individuals but not to others. The second theory emphasizes that privacy is to be alone. This confuses privacy with solitude. We can have privacy without being alone.

While these two theories focus on physical privacy or accessibility privacy, the two remaining theories focus on information privacy. The third theory is about control, specifically the control of information about ourselves. This is the type of theory that Cavoukian proposes [1]. According to Tavani, this type of approach confuses privacy with autonomy. One cannot autonomously reveal all information about oneself and still reasonably be said to retain privacy. The control theory misses something important, namely restricted access to information. This aspect is highlighted by the fourth view. Privacy is at hand when access to information about an individual is restricted in certain contexts. However, this view underestimates the role of control or choice. The individual must have at least some control of information about himself or herself. Moreover, it runs the risk of confusing privacy with secrecy, because it seems to imply that the more information about oneself is hidden, the more privacy one has [18].

As an alternative to these four theories, Tavani suggests a theory of "restricted access/limited control". It contains elements from the theory of restricted access and the control theory. Privacy is understood in terms of restricted access to information about an individual in a particular situation, but also in terms of limited control of this information by the individual. There has to be some restriction in access and also some control by the individual, but how much restriction and how much control by the individual depends on the context. This focus on context is the key point of the model [18]. Here Tavani is influenced by Nissenbaum who introduced the concept of "contextual integrity". Contextual integrity is respected if the following two types of norms are followed and violated when any of them is not followed: norms for the appropriateness of certain information (what information is appropriate to disclose in a particular context) and norms for the flow or distribution of certain information (each sphere in society has its own unique set of norms for fair distribution) [8].

Other philosophers defending similar conceptual views in the debate on the ethics of information and communications technologies are Moor [7] and Volkman [19]. Each proposes some kind of combination of restricted access and limited control. Given the arguments above, it seems that such a combined approach is preferable to Cavoukian's control theory.

In issues of privacy it seems reasonable to consider both aspects of restricted access and aspects of control. Moreover, in discussions of privacy by design in personal health monitoring different levels of access and different levels of control are precisely what need to be in focus. Privacy is a gradual concept. We can have more or less privacy. The very terms "restricted" and "limited" indicate that there can be different degrees or levels of privacy.

Implications for Privacy by Design

Let us investigate the implications of the three theories of information privacy for privacy by design.

One could reasonably expect that Cavoukian's control theory of privacy would imply that privacy in this sense should be built into design. However, a control theory of privacy seems, at least at first glance, incompatible with automatic data protection built into design. If the level of protection is automatic, it cannot be chosen by the individual as one option among others—other than the option of not using the technology at all—and if it cannot be chosen by the individual as one option among others, it is not controlled by the individual. Conversely, if the level of protection is controlled by the individual, it has been chosen as one option among others, and if it has been chosen as one option among others, it is not automatic. However, perhaps Cavoukian has another interpretation of the concept of control, one that is compatible with automatic data protection? One possibility is the idea that the user gains control by accepting the predetermined restricted access made possible by the built-in design. The user wants restricted access and gets it automatically, and then feels as being in control, despite the fact that he has not chosen the level of protection himself as one option among many others; he has only chosen the option of using the technology rather than not using it. However, if this is control, it seems to be very limited, indeed.

I do not rule out this latter interpretation of control, but if Cavoukian wants automatic data protection, a restriction theory of privacy seems more appropriate than a control theory. This type of theory is not necessarily linked to control by the individual user. The level of restricted access can be decided by the individual user of the technology, but also by programmers (by algorithms), controllers (by decisions within an organisation), or politicians (by legal regulation). It should be noted that in the European Commission's proposal it is stated that the "controller" should see to it that data are minimized—the automatic level—not the individual user.

A privacy theory of "restricted access/limited control" is compatible with both automatically determined data protection levels and data protection levels chosen by the individual user. As pointed out above, I support such a combined theory of information privacy. However, adopting such a theory does not by itself determine the issue as to what extent privacy by design should be used to protect information privacy. Let us now turn to this issue.

Broad Privacy by Design and Narrow Privacy by Design

Cavoukian argues that design should aim at preventing all harm-generating behaviour. To effectively prevent harm-generating behaviour data protection should be built into the technology. She states:

> PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred–it attempts to *prevent* them from occurring [1]; "PbD" means privacy by design).

This approach focuses on automation, relating in particular to principles (2), (3) and (5) in Cavoukian's list. Data should be automatically protected in all data handling from beginning to end. All harm-generating behaviour should be prevented by technological design. For this reason, let us call this version of privacy by design "broad privacy by design".

There are at least two important arguments in favour of this version. They are closely linked. The first argument focuses on security and effectiveness. Information can be very sensitive—this holds true especially for health information—and we cannot leave it to the unreliable human factor to protect it. It has to be standardized and automatized to provide secure and effective protection [1]. The second argument emphasizes that many people lack sufficient IT skills to protect their own sensitive information. It is difficult to get protection in today's complex world of information and communications technologies without privacy by design. This is how Schaar articulates this argument: "many users have only limited IT skills and hence are not in a position to take relevant security measures by themselves in order to protect their own or others' personal data" [16].

Pagallo proposes a view that differs radically from broad privacy by design [12, 13]. He argues that data protection should not be built into the technology to avoid all harm-generating behaviour. Design should rather be used to encourage people to change their harm-generating behaviour or reduce the impact of harm-generating behaviour (cf. [20]). This is how Pagallo expresses this idea:

> I suggest abandoning the idea of making data protection automatic by design, so as to prevent every harm-generating conduct from occurring. Rather, we should focus on other mechanisms we may aim at through design, that is, both the aim to encourage the change of people's behaviour via user friendly interfaces and to decrease the impact of harm-generating conducts through "digital air-bags" as encryption and other security measures [13].

Pagallo presents several arguments. First, he stresses certain difficulties. Privacy by design is difficult to implement because different values—for instance, different views on privacy—may have different impacts on the features of design. For example, should we have an opt-in or an opt-out model? Should patients' names be separated or not from data on health status and medical treatment? Moreover, it is difficult to achieve total control by legal regulation, so it may actually be the programmers that will control the data protection. Finally, it is technically difficult to safely balance different levels of control and access via software [13].

Pagallo's key argument, however, is that automated data protection limits autonomy. He states:

> … it is undisputable that the more personal choices are wiped out by automation, the bigger the threat of modelling social conduct via design …
>
> Instead of letting people determine autonomously levels of access and control over personal data, depending on personal choices and circumstances, the use of self-enforcement technologies seems incompatible with … autonomy [13].

Pagallo stresses principle (7) among Cavoukian's principles, i.e., respect for the individual user. He describes his approach as a "stricter" version of privacy by design, presented "in the name of individual autonomy" [13]. This version is stricter in the sense that design is only to be used to encourage people to change their harm-generating behaviour (by user-friendly interfaces) or reduce the impact of harm-generating behaviour (by various security measures such as encryption), not to prevent all harm-generating behaviour. Let us call this more modest version "narrow privacy by design", in contrast to Cavoukian's "broad privacy by design" (which aims at preventing all harm-generating behaviour). While broad privacy by design is characterized by automatic data protection, narrow privacy by design is characterized by autonomously chosen data protection.

A Middle Road Based on the Theory of Restricted Access and Limited Control

Which version is to be preferred, broad privacy by design (the automation version) or narrow privacy by design (the autonomy version)? Let me start with a brief comment on Cavoukian's version, namely that although privacy by design looks promising in many fields, Cavoukian seems too optimistic. Dix, for example, argues that there are no simple technical solutions of privacy issues. This is how Dix expresses this view:

> It is now important to focus on designers and manufacturers of technology in order to build privacy protection as far as possible into the systems from the start. However, such systemic data protection should not be mistaken for the magic "privacy button." There is and there will be no such thing. Privacy by design is no panacea because there is no simple technical fix for complex privacy challenges, but without privacy by design, it will be difficult if not impossible to achieve meaningful privacy protection in the twenty-first century [2].

Dix stresses that there is "no simple technical fix". Although we should build data protection into the technology "as far as possible", it might not solve all problems. On the other hand, Dix also states that it will be almost impossible to achieve privacy protection without privacy by design. So, privacy by design should be used as far as possible to protect information privacy, but it will never be sufficient. Dix seems to defend broad privacy by design but in a slightly weaker sense than Cavoukian.

Pagallo highlights various difficulties with broad privacy by design. However, these difficulties do not regard what is basically at stake, i.e., automation versus autonomy, but concern more pragmatic aspects. I agree that there are different views on values and that these views may have different implications for the type and level of protection. However, the European Commission's proposal indicates that it is possible to reach some consensus on the importance of data protection by design. Moreover, I agree that legal regulation is difficult, but, again, the European Commission's proposal indicates that such regulation to some extent is possible. What about technical difficulties? Even these may be possible to solve, at least to some extent. In some cases, for example regarding sensor technology, it seems rather easy to achieve privacy by design in terms of data minimization. In other cases, for example regarding the use of social media, privacy by design is secured, for example, in terms of passwords (see further below). Encryption is also a possibility. However, it is still an open question to what extent technological solutions to privacy issues are possible.

Pagallo's key argument—the argument from autonomy—is, at least at first glance, strong. In assessing his argument it is vital to note that autonomy can be exercised at different levels:

1. To choose autonomously whether or not to use a system with in-built privacy by design,
2. To choose autonomously which information is to be collected and transmitted,
3. To choose autonomously how the information is to be processed and used, and
4. To choose autonomously who should have access to the protected information and what level of access.

Pagallo seems to aim at autonomous choices at level (2), (3) and (4) and regards option (1) as no real choice at all; either you accept the system or not. Cavoukian, on the other hand, aims at autonomy at levels (1) and (4). In discussing one particular device (GE's QuitCare), she states that "the privacy features are fully integrated into the system, and cannot be removed or deactivated by the user" [1]. This indicates that the user has no autonomy regarding which information is to be collected, transmitted, processed and used [options (2) and (3)]. Either you choose autonomously to use the system or not [option (1)]. But Cavoukian also says that "the responsibility for determining access rights to a particular individual's information belongs to the care provider in consultation with the individual" [1]. This indicates that the user should have some influence on who should get access and the level of access, i.e., at least some limited autonomy [option (4)]. Pagallo and Cavoukian seem to agree on the importance of option (4). The key question is how important it is to be able to choose autonomously which information is to be collected and transmitted in the first place [option (2)] and to be processed and used [option (3)]. To Pagallo this seems to be of vital importance; without this option we cannot talk about autonomy in a true sense. Cavoukian, on the other hand, thinks that this is less important. To her, it is more important to have a guarantee that one's privacy is protected, and the most secure and effective way to achieve this is to make data protection automatic.

In discussing these issues it is vital to notice that privacy may carry different weight for different individuals in different contexts. Young and healthy people, for example, may be very sensitive while frail older people may not, because health and safety are more important to them than privacy. The importance of privacy in general and of privacy by design varies among individuals and varies from one context to another. Privacy by design may not be so important in some cases, but very important in others.

With this in mind, it is important to be clear about why privacy is important and when. Here I think that Rachels' [14] seminal paper on this issue is particularly enlightening. Rachels begins by showing that violation of privacy can in some unusual situations lead to people feeling embarrassed, being disadvantaged or even discriminated, but stresses that what is important more generally in ordinary situations is that some information about a person simply is nobody else's business. What is somebody else's business depends on the kind of relation the two persons have and on the particular situation [14]. This focus is also stressed by Nissenbaum. It is the relationships, social roles, contexts and situations that determine what information about a person it is appropriate that another person gets and how he gets it, how it flows and is distributed [8]. For example, we may want to disclose certain information to a friend but not to a bank man. But it could also be the other way around. We might want to disclose some information to the bank man but not to our friend. Similarly, we may want to disclose certain information to our physician, but not to our neighbour [14].

So, the problem is how to find a reasonable balance between automatic privacy protection and autonomously chosen privacy protection, a balance that is context-sensitive. In order to find such a balance it is necessary to have an adequate theory of privacy, and it is the combined theory of restricted access/limited control—rather than the control theory or the restricted access theory—that provides this option. We may need some automatic data protection as well as some autonomously chosen data protection, and this is precisely this context-sensitive approach that the theory of restricted access/limited control offers.

My conclusion is that Pagallo overstates the importance of autonomous choices and that Cavoukian is too simple-minded in pointing out the benefits of automation. I suggest a middle road. In some contexts, it is vital with several options regarding the level of protection. Here "one-size-fits-all" is not appropriate. Take the example of burglar alarms for private houses. The house owner has several options. One is to not have any alarm whatsoever. However, if he wants an alarm there are different degrees of protection, i.e., different alarms, at various prices. In other contexts, it is not vital with several options. The "one-size-fits-all" approach seems quite appropriate. Take, for example, privacy protection at a hospital. Electronic medical records need certain common standards. There cannot be different levels of privacy protection for different patients. Since health information may be perceived as particularly privacy sensitive by some patients and since we do not know exactly who they are, it has to be protected for everyone. It seems that Pagallo's approach is not sufficiently context-sensitive.

After this general discussion, let us turn to privacy issues in personal health monitoring.

Restricted Access and Limited Control in Personal Health Monitoring

What does the theory of restricted access/limited control imply for personal health monitoring? Here are two important advantages regarding privacy in this sense of personal health monitoring at home compared to staying at a hospital or nursing home:

- Others have restricted access to the patient's life. When the patient by using the personal health monitoring technologies can stay longer at home, he avoids being seen or heard by other patients, as he would if he shares a room in a nursing home or hospital.
- The patient has control over what access others have to his life. When the patient can stay longer at home he can more easily determine who he shall meet and who shall get information about him than if he shares a room with others at a nursing home or hospital [3].

While stressing both these aspects, Essén argues that we should add one more aspect that has been neglected in the literature on monitoring:

- The patient has restricted access to the lives of others. By staying longer at home, the patient doesn't need to see or hear other patients, as would be the case if he shares a room with others at a nursing home or hospital [3].

However, even if the patient is able to stay longer at home due to personal health monitoring and this has certain advantages with regard to privacy, personal health monitoring may in and by itself give rise to privacy issues. Let me give a few examples.

- Electronic medication assistance technologies help the patient to take the right medicine, in the right dose, at the right time. If the information is transmitted to the care provider and unauthorised people get access to it, it might be privacy intrusive, perhaps especially so regarding medicines for mental disorders, which may be considered a particularly sensitive matter in society.
- Health information from sensors monitoring heart failure or glucos levels, whether worn on the body or implanted into the body, may be privacy sensitive.
- Sensors for fall detection and motion detection in old patients' homes may be perceived as privacy intrusive by the patients but also by visiting relatives and friends who will also be detected.
- Night vision cameras monitoring whether the patients stay in bed are likely to be considered by some as very privacy intrusive.
- Night vision cameras in nursing homes controlling who is walking around in the corridor at night may be a sensitive matter.
- Mobile safety alarms with GPS positioning and geographic fencing for somewhat demented persons (signalling if they have walked outside a predetermined geographic area) might also be considered privacy sensitive.
- Internet portals for relatives giving them opportunity to monitor the welfare of elderly people by receiving information from reminder panels—for example, that a window is not closed or a hotplate is not turned off—might be privacy

intrusive to the elderly person, especially if the relatives are overprotective, overly worried or have an excessive need to control. The relatives might want access to more information than the elderly person really wants.

- The internet can connect patients or elderly people with relatives or care providers by means of computers, screens on walls or robots with mobile screens following the person through the apartment ("skype on wheels"). This kind of monitoring can be privacy sensitive. Social media like Facebook may connect people but also be privacy sensitive. The possibility of information about which web sites have been visited may also be sensitive.

Here Rachels' distinction between privacy issues in extraordinary ("unusual") situations and in ordinary situations is relevant [14]. In some extraordinary situations some patients may be harmed in personal health monitoring without sufficient data protection. For example, information from personal health monitoring may be more sensitive for a celebrity than an ordinary person. Similarly, young people might be more sensitive than old people. Some older people may not bother. For them safety is more important than privacy. Young people with chronic illnesses may be of a completely different opinion. For them a private sphere may be extremely valuable. Moreover, when younger family members visit their elderly relatives, some of them might be disturbed by knowing that they are also being monitored by various sensors. For a refugee with bad experiences of surveillance personal health monitoring may bring back terrible memories. For people with socially stigmatising diseases or disorders—for example sexually transmitted diseases or mental disorders—transmission of health data may also be especially sensitive. But who might want to get unauthorised access? Who would be interested in the personal health information? Is personal health monitoring really a threat to privacy? Most people are, of course, completely uninterested. However, there might be people working at healthcare centres that are interested in neighbours, journalists that are interested in celebrities, relatives that are overprotective and worry too much who want more information, hackers that just want to hack for fun or to show that it is possible to hack and so forth. So, there might be some people that behave in a privacy intrusive manner.

What about privacy issues in ordinary situations? We saw that Rachels stresses that what is important more generally in ordinary situations is that some information about a person simply is nobody else's business. What is somebody else's business depends on the relation and the situation [14]. This is highly relevant to personal health monitoring. Privacy is important in personal health monitoring because we may want to disclose health information to our physician, but perhaps not to other health professionals working at the same healthcare centre, neighbours, journalists or (sometimes) even our relatives. The health information that is collected and transmitted is simply not these peoples' business.

How Can Privacy by Design Be Applied in Personal Health Monitoring?

The problem arises how to respect privacy in personal health monitoring. Can the concept of privacy by design be applied? If so, how? Regardless of whether one accepts broad privacy by design, narrow privacy by design or a middle road, it is possible to accept certain automatic data security measures. Two problems are particularly important to address:

1. Which information is to be collected and transmitted in the first place?
2. Who should have access to the information and what level of access?

In the proposal by the European Commission mentioned above we get some indication of how problem (1) can be addressed:

> The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage [4].

This statement seems to propose the following conditions:

1. Only collect and transmit data for a specific purpose.
2. Only collect and transmit data that is necessary for this purpose.
3. Do not collect, transmit and keep data beyond the minimum necessary for this purpose (see also [6, 11].

The proposal by the European Commission also gives an indication of how to address problem (2). It states:

> In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals [4].

However, here it seems that the proposal is much too weak when applied to personal health monitoring. Here it is not a matter of not making the information accessible to "an indefinite number of individuals" but of making it accessible to a definite number of individuals, namely only to physicians and other health care professionals that are directly involved. Therefore I propose the following fourth condition:

4. Only provide access to the data for those health care professionals who are necessary for this purpose.

How can this data minimization by design and restricted access by design be implemented in practice in personal health monitoring? Let us return to the examples above (in investigating these issues I have received valuable input from Steven Savage (personal communication)).

- Electronic medication assistance. If a doctor wants to monitor an old patient to check whether he has taken his medicine, she could ask: has he taken his medicine for heart failure and high blood pressure, his sedatives, his diuretic medicine and so forth? But the information the doctor really needs is: has the patient taken his medicine? The answer is then either "yes" or "no". The information that should be collected and transmitted is then "yes" or "no". In this way the risk for privacy intrusion is minimized. Even if somebody would get unauthorized access to it, this would be relatively unproblematic, because the context is lacking.

- Monitoring heart failure, glucos levels and so forth by means of sensors that are worn or implanted. One option would be to only transmit information if something extraordinary happens, rather than continuously, and then only such neutral information as that the patient should be asked to come to the health care centre for control within a certain number of days or hours. As in the previous case, if somebody would get unauthorized access to the information, this would be relatively unproblematic, because the context is lacking.
- Fall detection and motion detection by sensors in the patient's home. Here the focus may be on anomalies only. In the case of fall detection, information will be transmitted only when the patient has fallen and then only in terms of a "yes". In the case of motion detection information will be transmitted only when the patient has not moved for a certain period of time in contrast to the general behavioural pattern and then, again, only in terms of a "yes". In this way the risk for privacy intrusion is minimized due to lacking context.
- Night vision cameras monitoring whether the patients stay in bed. Some privacy protection could be provided by means of an infrared camera, since the quality of the picture is rather bad. Another option is to "blur" the picture.
- Monitoring in a nursing home at night to see if somebody is moving around in the corridors. In order to protect privacy this could also be done by means of infrared cameras, since the quality of the pictures is not sufficiently good to identify a person, but sufficiently good to identify that somebody is moving around. Another option, also in this case, is to "blur" the pictures. If one wants to know whether somebody is going in or out of a room, one could use a camera, but one could also use a pressure mat with a sensor in the doorway. The former alternative would give a lot of unnecessary surplus information that could be privacy intrusive, while the latter would only give information about what one really wants to know, i.e., whether somebody went in or out.
- Internet portals for relatives giving them opportunity to monitor the welfare of elderly people by receiving information from reminder panels. By passwords it is secured that only relatives have access.
- Mobile safety alarm with GPS positioning and geographic fencing for a somewhat demented person. Access is protected by passwords.
- Internet connection to promote social contact with relatives by means of computers, screens on walls or robots with mobile screens. Even in these cases access is secured by passwords.

It should be noted that in at least some of the above cases, encryption is also a possibility.

Should Privacy by Design Be Applied in Personal Health Monitoring?

We have seen that the concept of privacy by design *can* be applied to personal health monitoring to resolve privacy issues raised by this technology. Now the question arises: *Should* it be applied in personal health monitoring? There are several arguments in favour.

First, automatic data minimization in collection and transmission may minimize the harm of unauthorized access. By limiting what is being processed the damage of data loss will be limited. If data is accessed without authorization it would not say much if it consists only of information in terms of “yes” or “no”, since the context of this “yes” or “no” is lacking. Moreover, if more comprehensive data amounts are accessed without authorization but the data is encrypted, it will do no harm, either.

Second, personal health monitoring concerns health and therefore the standard privacy protection in regular health care should also be the standard in this health activity. We cannot have different rules for different patients in different types of care. All health information can be sensitive, and all patients whether monitored at home or at a hospital should have the same protection.

Third, since health information may be sensitive, it is particularly important to protect. If privacy is securely and effectively protected by design and this automation to some extent reduces autonomous choice, this price is acceptable to pay.

Fourth, data minimization, as a key aspect of privacy by design, is likely to be uncontroversial regarding health data. Who would like unnecessary health information to be collected and transmitted? The problem is rather to determine what is necessary and what is not, given a particular purpose.

Fifth, for many elderly patients privacy is not as important as safety. Their privacy can preferably be protected by design. They should not have to consider by themselves various privacy protecting options. They have not real interest in bothering themselves with autonomous choices regarding different options.

I accept these arguments. Privacy by design in terms of in-built data protection has a clear potential to protect privacy in personal health monitoring, at least to some extent. However, there are at least two important con arguments to be considered.

First, privacy by design is not sufficient for protecting privacy in personal health monitoring. Privacy by design cannot solve all privacy problems with the handling of data. Examples are the management of the transmitted information, the decisions on what to do based on the information that ultimately must be made by the medical staff, and the issue of who shall have access to the data. Even if privacy by design is part of the whole lifecycle of data-processing, including operation, management and access, it is not sufficient for these aspects. There is always a need for responsible handling of the data by human agents. This requires policies, training, procedures and incident management.

The second argument is the autonomy argument, which we have met in a more general form above. Patients should have various options to choose among autonomously. There should be no “one-size-fits-all”, but patients should have the opportunity to choose a higher or lower level of protection. Only in this way health monitoring can be truly “personalized”.

These con arguments do not carry sufficient weight to abandon the idea of privacy by design, but they indicate two kinds of limitation:

1. Privacy by design cannot solve all privacy problems. Responsible handling of information by human agents is always of vital importance.
2. Autonomy. Although automated data protection is useful in many contexts, it is not desirable in all contexts. In some contexts, the possibility of autonomous choice of the level of protection might be more important.

To What Extent Should Privacy by Design Be Applied in Personal Health Monitoring?

None of the pro arguments clarify to *what extent* the concept of privacy by design should be applied in personal health monitoring. They only give us reason to believe that it should be used to some extent. Neither do the two types of limitation indicated by the con arguments specify the extent to which it should be used. What would the middle road between broad and narrow privacy by design imply? It implies that in order to find a more precise answer to the question of extent we need to distinguish different contexts of monitoring.

In some contexts like medication assistance and monitoring of specific health parameters such as heart failure or glucos levels, one single automatic option is legitimate (see above). However, regarding some other contexts of monitoring a multi-choice approach stressing autonomy is warranted. The user has a possibility to choose which parameters to be monitored. This holds true especially regarding monitoring in which relatives are the receivers of the health-relevant information rather than health professionals. A key example is the Internet portal for relatives which gives them possibility to monitor the welfare of elderly people by receiving information from reminder panels. It should be noted that in this case the information is not health information in the narrow sense, but only health-relevant information about, for example, whether windows are closed or hotplates turned off. The information is health-relevant because if windows are not closed and hotplates not turned off this may cause health problems. In this way the information may be used for prevention of health problems and securing the welfare of the elderly. It seems reasonable to provide the elderly person and her relatives with several options regarding what to monitor and to what extent the relatives should have access to this information. Privacy is protected by passwords—so there is privacy by design—but the level of access is chosen by an agreement between patient and relatives. The same holds true for information to relatives from mobile safety alarms with GPS positioning and geographic fencing. A plurality of options to choose among is also reasonable regarding elderly peoples' use of social media. The users can decide what to disclose and what not to disclose. However, privacy by design is provided in terms of passwords.

Concluding Remarks

We have seen that values play a central role in privacy protection. There are different views on how privacy should be conceived and how significant it is.

Moreover, there are different views on how privacy by design should be conceived and to what extent it should be used, generally and more specifically in personal health monitoring.

I have assumed a privacy theory of restricted access/limited control. On the basis of this theory, I have suggested a version of the concept of privacy by design that constitutes a middle road between what I have called broad privacy by design and narrow privacy by design. The key feature of this approach is that it attempts to balance automated privacy protection and autonomously chosen privacy protection in a way that is context-sensitive.

In personal health monitoring, this approach implies that in some contexts like medication assistance and monitoring of specific health parameters one single automatic option is legitimate, while in some other contexts, for example in monitoring in which relatives are the receivers of the health-relevant information rather than health professionals, a multi-choice approach stressing autonomy is warranted. The patient should have a possibility to choose which parameters to be monitored and the level of protection.

In a nutshell, the concept of privacy by design has potential, but also certain limitations. One limitation is that technological design cannot provide complete privacy protection. Responsible handling of data by health care professionals is always necessary. Another limitation is that complete automation is not desirable from the perspective of individual autonomy. Depending on the context, there should be room for some autonomous choice of protection levels.

Acknowledgments Research for this paper was funded by the European Commission (the project "Personalized Health Monitoring – Ethics" (PHM-Ethics); contract number 230602) and New Tools for Health (VINNOVA, Sweden).

References

1. Cavoukian, A., Fisher, A., Killen, S., & Hoffman, D. (2010). Remote home health care technologies: How to ensure privacy? Build it in: Privacy by design. *Identity in the Information Society, 3*(2), 363–378.
2. Dix, A. (2010). Built-in privacy–no panacea, but a necessary condition for effective privacy protection. *Identity in the Information Society, 3*(2), 257–265.
3. Essén, A. (2008). The two facets of electronic care surveillance: An exploration of the views of older people who live with monitoring devices. *Social Science and Medicine, 67*(1), 128–136.
4. European Commission. (2012). Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Brussels.
5. Finkelstein, S., Speedie, S., & Potthoff, S. (2006). Home telehealth improves clinical outcomes at lower cost for home healthcare. *Telemedicine and e-Health, 12*(2), 128–136.
6. Langheinrich, M. (2001). Privacy by design—principles of privacy-aware ubiquitous systems. http://cs.gmu.edu/~jpsousa/classes/699/papers/privacy%20Langheinrich.pdf. Accessed May 30, 2013.
7. Moor, J. H. (1997). Towards a theory of privacy in the information age. *ACM SIGCAS Computers and Society, 27*, 27–32.
8. Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*(1), 119–158.
9. Noel, H. C., Vogel, D. C., Erdos, J. J., Cornwall, D., & Levin, F. (2004). Home telehealth reduces healthcare costs. *Telemedicine Journal and e-Health, 10*(2), 170–183.
10. Nordgren, A. (2012). Remote monitoring or close encounters? Ethical considerations in priority setting regarding telecare. *Health Care Analysis*. (advance publication online). doi:10.1007/s10728-012-0218-z.

11. OECD. (1980). Guidelines on the protection of privacy and transborder flows of personal data. http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Accessed May 30, 2013.
12. Pagallo, U. (2011). Designing data protection safeguards ethically. *Information, 2*, 247–265.
13. Pagallo, U. (2012). On the principle of privacy by design and its limits: Technology, ethics and the rule of law. In S. Gutwirth, R. Leenes, P. De Hert, & Y. Poullet (Eds.), *European data protection: In good health?* (pp. 331–346). Heidelberg: Springer.
14. Rachels, J. (1975). Why privacy is important. *Philosophy & Public Affairs, 4*, 323–333.
15. Rössler, B. (2005). *The value of privacy*. Cambridge: Polity Press.
16. Schaar, P. (2010). Privacy by design. *Identity in the Information Society, 3*(2), 267–274.
17. Solove, D. J. (2002). Conceptualizing privacy. *California Law Review, 90*, 1087–1155.
18. Tavani, H. T. (2007). Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy, 38*(1), 1–22.
19. Volkman, R. (2003). Privacy as life, liberty, property. *Ethics and Information Technology, 5*, 199–210.
20. Yeung, K. (2007). Towards an understanding of regulation by design. In R. Brownsword & K. Yeung (Eds.), *Regulating technologies: Legal futures, regulatory frames and technological fixes* (pp. 79–108). London: Hart Publishing.