Privacy and Future Consent in Smart Homes as Assisted Living Technologies

Erik Thorstensen(✉)

OsloMet—Oslo Metropolitan University,
PO box 4 St. Olavs plass, 0130 Oslo, Norway
erik.thorstensen@oslomet.no

Abstract. In the field of assisted living technologies, one central strand is to investigate how smart homes might fulfill ambitions for older adults to live longer at home. With the advent of the General Data Protection Regulative (GDPR), there are clear regulations demanding consent to automated decision-making regarding health. This contribution to applied ethics in the field of algorithmic decision-making opens up some of the possible dilemmas in the intersection between the smart home ambition and the GDPR with specific attention to the possible trade-offs between privacy and well-being through a future case, to the learning goals in a future smart home with health detection systems, and presents different approaches to advance consent.

Keywords: Privacy · Consent · Responsible innovation · Applied ethics
Algorithmic decision-making

1 Introduction

This paper presents reflections based on a current research project developing Responsible Research and Innovation (RRI) in the field of assisted living technologies [1]. There are two main sources of background to this paper. The first is the ambition in the project to develop smart homes for older adults that can assist them in residing longer in their homes by introducing decision support and aid when cognitive functions decline. The second source of inspiration is the novel European General Data Protection Regulative (GDPR), which becomes effective as of May 25, 2018.

In order to develop these reflections, I will begin with a presentation of RRI and the ambitions of the research project as well as thoughts on smart homes as assisted living technologies, before moving into the GDPR and how our current use of informed consent might be challenged by smart devices and smart homes. Before moving onto an example case that I have constructed, I briefly touch upon the meaning of privacy in this paper and set out to analyze the case as a contribution to the ethics of assisted living technologies and not as a contribution to the rich legal debate on the GDPR (e.g. [2–4]). The analysis is in three interrelated parts: one discusses privacy, health and consent; the second probes lightly into combined economic and normative challenges of smart homes as health systems; and the last looks further into the issues of future consent.

J. Zhou and G. Salvendy (Eds.): ITAP 2018, LNCS 10927, pp. 415–433, 2018.
https://doi.org/10.1007/978-3-319-92037-5_30

2 Responsible Research and Innovation

Responsible Research and Innovation (RRI) is an approach to research and research policy that aims at articulating socially beneficial impacts in order to steer research and innovation towards such impacts rather than blindly towards monetary gain [5, 6]. It is then a proactive approach to achieve positive goals by innovation, rather than trying to minimize damage. Consequently, there is some form of anticipation of the future involved. Even if we cannot know the future, all individuals have some form of vision of what they believe will happen and these visions might be assessed [7]. Richard Owen et al. have described anticipatory activities as "describing and analyzing those intended and potentially unintended impacts that might arise, be these economic, social, environmental, or otherwise" [8, p. 38]. Different forms of anticipation might serve as a basis for a discussion on the state of knowledge regarding what actions one should take in order to achieve the positive goals – or being deliberative, reflective and responsive, as Owen et al. would phrase it. This contribution is definitely within the field of anticipation with the aim for future deliberation and responses to a not unlikely scenario.

The research and innovation project includes researchers from the health professions, ICT, and ethics – as well as a medium size enterprise developing smart homes and assisted living technologies, a residence complex for older adults and a governmental body in the project. There are two aims to the project: (1) develop and test important elements from RRI beyond the state of the art; and (2) develop and test smart home-like features in the homes of older adults based on different sensor input processed by machine learning techniques with the aim of providing advisory outputs [1].

3 Smart Homes as Assisted Living Technologies

A common understanding of assisted living technologies is "any item, piece of equipment, or product system, whether acquired commercially off the shelf, modified, or customized, that is used to increase, maintain, or improve functional capabilities of individuals with disabilities" [9, p. 1]. Smart homes is a term designating "a residence equipped with a communications network, linking sensors, domestic appliances, and other electronic and electric devices, that can be remotely monitored, accessed or controlled" [10, p. 362]. Such residences have in the last 25 years been seen as a facilitating for independent living of older adults, that is becoming assisted living technologies [11]. Currently, smart homes are controlled by means of the voice, smart phone apps or switches. Janienke Sturm suggests that smart houses might be used to encourage healthier behavior and contribute to saving energy [12], while empirical work indicates that the users might be more interested in having visitors and fun [13]. In addition to identified ethical concerns [14], one central challenge in applying a smart house concept as an assisted living technology is the possible (future) connection to health services. For security and privacy reasons, the health services' databases and infrastructure are not currently connected to commercial monitoring systems. In the current project, data are collected from a series of binary (on/off) sensors in each apartment, typically a movement sensor in each room, magnetic sensors on doors, and

power sensors on some appliances. The data are processed using machine-learning with the aim to provide improved smart-home functions that adapt automatically to the preferences of the individual resident.

In an ambition to create diagnostic home environments, Nijhof et al. successfully tested a system designed for persons with dementia to give early warnings for deterioration in their condition [15]. It further increased the residents' and informal caregivers' feelings of safety and security and seemed to reduce the strain on the health professionals. Even though the current scientific evidence for smart houses as effective tools in assisting older adults to remain at home is weak [16], the potential benefits from developing diagnostic systems built into smart houses seem only to be limited by one's imagination – in addition to the state of the art in medical diagnostics [17]. However, as this paper will address, there are new and changing configurations of the role of consent, professional practice and normative concerns that need to be addressed for this transition to be successful.

4 The General Data Protection Regulation

From May 25, 2018, the legislation on collection, processing, storage and distribution of personal data in Europe is based on the General Data Protection Regulation (GDPR) Although this is not a paper in law, but rather in applied ethics, the GDPR nevertheless provides an important ethical case. Articles 13 and 14 (addressing processing of personal data for automated decision-making) state that a person has the right to "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject" in making a decision for or about a person that concerns "performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements" [18, article 4 (4)]. According to Goodman and Flaxman's reading of the new EU regulations, all algorithmic decisions affecting a subject's health need to be explained to the person concerned [3].[1]

Furthermore, the GDPR demands that new devices will have a maximum privacy as a default setting – so called "privacy by default" – as articulated in Article 25 of the new legislation, which highlights the issues of purpose specification and data minimization for personal data collection.

It seems then that there might be a conflict between the provision of decision support through smart homes (or any smart device) and the understanding clause in the GDPR. In addition, the provision of maximum privacy settings on novel devices also seems to provide difficulties for technological artefacts that are explicitly obtained by a user in order to be used for collection of any set of personal (health and safety related) data, where the collection of such is not the artefact's primary purpose. This might conflict with the values or preferences of possible smart home users and also – potentially – endanger those in need of some kind of care if the settings are not in line with their expectations.

[1] Goodman and Flaxman's interpretation of the GDPR has been modified and challenged by legal scholars, see [2, 4].

The GDPR states that a data controller might be exempted from the prohibition on automated decision-making if this exemption is based on the "data subject's explicit consent" [18]. However, for data subjects to provide informed consent, they need to understand from what they as data subjects are exempting the data controller. Thus at some point there is an obligation for the data controller to explain this to the data subject, so that the data subject understands the scope and the content of automated decisions.

On the surface of it, this seems like a case for the courts. However, strategies for the legalization of societal issues run the danger of neglecting that political, commercial and civic notions of jeopardized rights might follow logics that differ from the legal logics emphasizing procedures based on individual legal rights or proportional harms [19]. Hence, an ethical assessment of the issues at stake might be a welcome contribution in order to spot if the different logics yield different outcomes.

Since reflection on future societal reconfigurations is an important part of RRI, we add a thought on distributive justice, were the information from smart homes to be used as a map for allocating health resources in the future.

5 Informed Consent and Privacy

If we look to the standard formulation of informed consent in bioethics as formulated by Beauchamp and Childress [20], understanding includes both the material information about the illness or disease and the reasons for choosing one plan instead of another

1. Threshold Elements (Preconditions)
   a. Competence (to understand and decide)
   b. Voluntariness (in deciding)
2. Information Elements
   a. Disclosure (of material information)
   b. Recommendation (of a plan)
   c. Understanding (of a. and b.)
3. Consent Elements
   a. Decision (in favor of a plan)
   b. Authorization (of the chosen plan) [20, p. 124]

With the ambition of providing decision support, and possibly automation of decisions, as a possible smart health services, both the disclosure and the recommendation phases might be left to machine operations. Such a change might well influence how we understand informed consent, and constitute a challenge to Beauchamp and Childress's version. A different approach to informed consent has been proposed by Onora O'Neill suggests that patient autonomy is conditioned by a professional's extensive knowledge [21]. In O'Neill's understanding, the ethical value of informed consent lies in a patient's assurance that there is no kind of deception or coercion involved in the research project or in the medical procedure suggested. O'Neill further proposes that such informed consent must be accompanied by the means for a patient to control the information (and its relation to the consequent actions) as well as easy ways

for withdrawing consent. If one were to view consent as involving some form of trusting relationship between a health professional and a patient, it seems then that the patient must be able to project some form of intent into a technological solution. Although there is evidence that people project intent into technologies [22], what the normative significance of such projections might be is still under debate, as for example in the discussion over robots' rights [23, 24].

One instance of such automated machine operations relevant to the current context might be that of machine-learning algorithms regarding suggestion for health interventions. Nicholas Diakopoulos explains this as, "[a]utonomous decision-making is the crux of algorithmic power. Algorithmic decisions can be based on rules about what should happen next in a process, given what's already happened, or on calculations over massive amounts of data" [25, p. 3]. In the context of algorithmic decision-making, Frank Pasquale temporarily concludes that "[t]ransactions that are too complex to explain to outsiders may well be too complex to be allowed to exist" [26, p. 16] in his book on financial algorithms. Furthermore, Omri Ben-Shahar and Carl E. Schneider have described how disclosure is becoming increasingly unrealistic because it demands expert knowledge for both the discloser and the disclosee, and because disclosure is a high-frequency phenomenon that we all encounter everywhere [27].

A related moral challenge in this field which is addressed in an early literature review by Päivi Topo, is that much assisted living technology for people with dementia has a bias towards the caregivers' needs and the studies supporting them did not include people with dementia themselves [28]. Several studies into a wide range of different stakeholders (including intended users) show that opposition to technologies is not founded in ignorance or value differences, but rather the simple fact that it is unclear what kind of benefit the technology provides for the stakeholder or user group in question [29–32]. Furthermore, if assisted living technologies do not provide goods for the weakest stakeholder group, which seems to be the older adults, then it is questionable if it is morally right for society to expose them to the risks from them [33]. Related to this, if there is a bias in the development and assessment of existing assisted living technologies towards caregivers' needs, it seems likely that smarter and automated solutions will inherit such bias with little human discretion to make corrections on the spot [34]. In sum, there seems to be little space for "a second opinion" with smart services.

Now, there are degrees to understanding automations. A medical doctor can be said to understand genetic therapy and suggest this as a course of action even if she or he is not able to perform medical genetics technology herself or himself. Likewise, there will probably be many instances of smart surveillance and alerts in future healthcare where the health professionals would qualify as understanding the basic ailments that a smart system is searching for and aiming at alleviating or preventing. However, in line with Responsible Research and Innovation, it is through looking for possible unexpected events and situations that the health system and society at large might create a more robust readiness for situations that would otherwise be surprises.

In this article I take as a point of departure Daniel Solove's taxonomy of privacy and follow him in the argument for a pragmatic understanding of privacy that extends beyond the "secrecy paradigm", where "privacy is tantamount to complete secrecy", and a privacy violation occurs when concealed data is revealed to others [35]. Solove's

approach which highlights the combination of non-hidden data seems very relevant for a period where the merger of different sources and registers constitutes the most relevant method for different forms of information dissemination and invasion. Solove has elsewhere argued that essentialist approaches looking for the necessary and sufficient conditions for a concept of privacy always seem to end up in conceptions of privacy which are either too broad or too narrow [36]. As an alternative Solove uses Wittgenstein's notion of *family resemblances* to tie together all the different uses and notions people have of privacy. For the purposes of this paper, it suffices to use Solove's classifications of informational privacy into *information collection*, *information processing*, *information dissemination* and *invasions*. I find Solove's classification useful when analyzing the following imagined case that highlights some of the socio-ethical dilemmas and problems that might arise with informed consent and automated decisions.

6 Oscar: A Near Future Case?

Fictions might on the one hand create unintelligible and incredible futures that squander our collective ethical resources [37], or can incite a discussion about what futures we want [38]. The proposed story has been discussed in several rounds, and I believe it highlights underlying normative issues.

We can imagine a case where a person, Oscar, lives alone at home and has some sensors and cameras connected to monitor burglary, heating, humidity, and fire as well as connection to GPS tracking, health monitoring and motion movements. They are all connected on his phone. Oscar is 81, he lives alone and he has two adult children, he frequents a social club for the older adults in his community, and he has a general practitioner (GP). Oscar has obtained a private security service through the social club that connects to the data from the phone. The security firm uses the same devices to deliver monitoring systems to the municipal health authorities, and there is a mutual understanding and a binding contract that the safety systems can be transferred to the public system when and if a legal decision has been made that Oscar is in need of a given type of care. The security and health system provides a choice between a binary rule-based system and a smart home machine learning system.

Oscar values his privacy so he has disabled the sensors for motion detection inside the house and only enabled the ones connected to intrusion. He has set the cameras to be triggered in case of intrusion, but also activated silhouette mode in order that natural pictures are triggered in case of falls. The camera has an internal logic, not connected to the smart home machine learning, in order to detect falls. However, Oscar also values his safety and this is the reason that he chose the firm that is compatible with the municipal services. He chooses the rule-based system.

Oscar then experiences forgetfulness and dizziness over a few days and he sees his GP. They agree that Oscar should connect the GPS tracking, health monitoring and motion movements from the phone to the municipal system and enable motion movement detection inside the house, but he keeps the cameras with fall detection to silhouette mode only, since he does not want to be filmed but only to receive help. He

switches to the smart home machine learning system and connects to the health delivery system in agreement with his GP.

One day Oscar discovers that his phone is no longer working properly so he buys one online, just as he has always done. The phone comes, in line with current regulations, with a maximum of privacy settings. Oscar does not read all the disclaimers from the phone producer, the operating system producer and the software providers. He installs his favorite apps as well as the apps to the surveillance system. He wishes to accept all the features in the surveillance system, but since these are presented as exceptions to the rule, Oscar does not feel comfortable in making such exceptions since he is not used to allowing for exceptions, and he has a general trust in decisions made by the phone in his daily life. The privacy settings are now no longer in line with Oscar's desires (and maybe even beliefs).

After a while, the settings are fixed, but the algorithm in the surveillance system has tracked the changes in Oscar's gait, sleep patterns and heart rate and found indications of changes in behavior consistent with forms of novel risks due to forgetfulness. The surveillance system then suggests increasing the amount of data gathered about Oscar in order to avoid dangers. However, the forgetfulness is accompanied by a loss in cognitive function, which makes it increasingly difficult to explain to Oscar and to ensure that he has understood how the system works.

6.1 Oscar – Informational Privacy Issues

Before moving into the broader discussion, it is important to spell out clearly what the informational privacy issues are that are at stake in the case above and who is responsible for these issues.

There are at least two parties who are responsible for the arrangement of the surveillance system: the system provider and Oscar. Furthermore, the health delivery system should also be counted among the agents. If we take as a point of departure that free will is not incompatible with determinism – whether or not determinism is true or not – then there are two conditions which are typically constitutive of an agent's responsibility, namely *knowledge* and *control* [39]. In the case of Oscar, his knowledge depends on the knowledge of the surveillance system provider and his control on their selected range of options. Now, knowledge or control are by nature gradual: we cannot have complete control nor complete knowledge, but we can on the other hand be ignorant and/or without control. In Oscar's case, this means that someone else, the surveillance provider and/or the health services, are in control. The supplier of the surveillance system is responsible for all matters of data security.

There are, I think, four relevant stages in the case of Oscar. The first, we can call *the procurement stage*, where he sets up the system and is in control and has limited surveillance; the second, which we can call *the dizziness stage*, where he connects the GPS and movements tracking; the third where he buys a new phone, which we can call *the phone procurement stage*; and the last which we can call *the illness stage* where the surveillance system takes on the role of GP.

The Procurement Stage
Oscar has entered into a contractual relation with the surveillance system provider, and thus subjected himself to some degree of external control over his home and his sphere of actions. He appears to wish to protect himself from physical intrusions; otherwise, he clearly wishes to limit the information collected about him since there are no activated sensors inside the house except the fall sensor in an anonymous silhouette mode. Information collection is a prerequisite for other types of information processing, and as he has selected the binary system, there is no processing of his different movements other than a trigger for falls. It seems reasonable to suggest that Oscar values being in charge of actions in his own house and deciding which form of intervention can take place.

The Dizziness Stage
Events have occurred that change Oscar's privacy preferences following a dialogue with his GP. He receives new knowledge about himself and he chooses to change the terms of the contract and the health service delivery becomes his new contract partner. He now has a range of data collected about him, and he knows that the data are processed in order to detect and diagnose possible changes in his health condition. Oscar knows which data are collected and the purpose for which these data are collected.

The Phone Procurement Stage
If Oscar is capable of buying a phone online, it seems that he is capable of providing valid informed consent. Based on research into digital privacy disclaimers, Oscar is not behaving any more recklessly than can be counted within the range of normal human behavior, and Solove argues that expectations constitute a central part of privacy (or violations of privacy) [35], in addition the understanding of privacy policies has become a field of research in itself (e.g. [40, 41]). So, in a case where the privacy settings for collecting personal information by default are not in line with a habituated user's expectations, one seemingly enters into a responsibility vacuum.

Now there are some imaginable solutions to such a strict collection practice, but they all have consequences for Oscar's privacy since this also increases the surveillance in earlier phases. First, the security system provider could provide a warning whenever a person changes a phone, and take action through the health delivery system in order to adjust the settings. However, this would also presuppose that the high level of privacy allows for information about phone changes to be sent from the phone provider to third parties, which might be or might not be the case. If one were to apply a strict version of the purpose specification principle, then it seems that the collecting of data about a specific individual's phone changes and transfer to the app's legal owner could constitute a form of secondary use of data.

Another solution could consist of making the health delivery system responsible for such technical follow-ups. This appears to be a good idea, but then again it places increased pressure on the health services and there is then the question of competencies in the professional system. If the findings of the studies on privacy settings are to be used as a point of departure, then there are few reasons to expect that any member of a health profession or a therapeutic profession will be able to enter into these settings in a competent manner. In the current context of smart homes adapted for health and

security use, it is not clear if any single profession might possess the adequate knowledge. According to Paul Faber, professional standards provide the foundation for a fiduciary relation between professionals and their clients [42]. Privacy settings and data safety and security in relation to declining cognitive functions is a complex affair that depends on the local data system (both hardware and software), on the user's life conditions, and the possible consequences of deteriorating cognitive capacities on this context. This seems to call for two types of solutions (or a combination of the two): (1) one could envisage transdisciplinary teams that work together in deliberating with the client (and among the professionals); (2) one could create a new type of professional with competence in ICT and health.

The Illness Stage

We believe that Oscar's phone has been set correctly. The next instance then occurs when the health surveillance system asks for expanded access to information about Oscar. Examples could be body temperature through the watch he has for GPS or through the surveillance camera, eye readings through his phone or the surveillance camera etc.

The two privacy issues here are that the machine could decide to collect more data. First, the making of such a decision is a form of invasion into what used to be the domain of the GP or Oscar – or both. Second, it is a question of the amount of data that is being collected. Third, it is the question of whether a general notion of "increased risk" should count as a legitimate reason for interfering with the traditional consent structure or what level of specificity should be given as a legitimate purpose for this increase – and this would also count for human data collectors. This theme will be further elaborated under the heading "future consent" below.

In what follows we will point towards some zones for possible controversy. Our general attitude to these dilemmas is that they should be opened up for discussion and debate since any form of easy solution seems questionable.

7 The Ethics of Normative Systems

In the case above, there are two central decisions that are outside of Oscar's sphere of action: (1) the forced maximized privacy settings; and (2) the smart surveillance system. These are two different instances of normative paternalism that point in different directions. The first instance is meant to reduce to a minimum the amount of information concerning Oscar as decided by a conglomerate of data gathering entities under the auspices of the phone manufacturer in combination with the providers of the operating system, most probably based on a logic towards privacy, based on risk reduction of the providers of the operating system and the phone manufacturer's bottom line. The second normative paternalism Oscar is subjected to is the smart surveillance system.

I assume here that the smart surveillance system contains an element of self-learning. It might well be a mainly rule-based or a hybrid system – or an entirely self-learning system. However, an algorithmic health surveillance system will (suggest to) perform actions that humans believe have normative force since they to some extent will be aimed at maximizing certain aspects of health, which many find valuable.

Implemented algorithms are implemented for a purpose. If one goes back to the wumpus world, the gaming-based imagined machine learning example by Stuart Russell, Peter Norvig and Ernst Davis [43], the agent has the goal of getting the gold (and avoiding being eaten by the terrible wumpus). The agent should maximize its score through a minimum of actions and a maximum of gold and thereby become close to a rational agent. However, there is a goal – and what might the goal be in Oscar's smart surveillance system?

The purpose of the algorithms could well be set in order to give precedence to the norm of minimizing maleficence for Oscar or for the health delivery system. This could on the one hand consist of the smart surveillance system prioritizing the detection of more probable incidents and reporting them, with subsequent increased intrusion into Oscar's home. An alternative underlying logic in the smart surveillance system might be directly adopted from maintenance of machinery, and thus follow cost-effectiveness analysis (CEA) logic where it is the severity in terms of harm reduction connected to monetary costs that underlies the learning logic in the smart surveillance system. In such a system what might be of no or little concern to Oscar but a potential huge cost to the health system – or huge concern for Oscar with little benefit from intervention –tilts toward deciding when to intrude into the home.

If we take as a point of departure Bonnefon et al.'s study of people's reaction to autonomous vehicles, one might create a form of the Prisoner's Dilemma from the two systems [44]. Bonnefon et al. found through a survey that while most people preferred that all self-driving cars should sacrifice one in order to save many, few people would buy a car that would sacrifice oneself in order to save more people. They then conclude that the most equitable and the overall preferred system will be a barrier to the introduction of self-driving cars – even if the total number of accidents seems likely to decrease with self-driving cars. If the same inclinations are present when it comes to the logic in a health monitoring system, then it seems reasonable to expect that most people would think that a health monitoring system should be based on equity, which would then be based on CEA for the distribution of resources. People would most likely prefer to have a maximum of protection for themselves – which again will decrease the overall societal benefit since this will result in a skewed distribution of resources.

As shown in Table 1, any single individual would benefit from a maximum of protection while society at large would lose. The benefit for the individual for any arrangement with skewed resources is larger than the relative cost for society because of the magnitude. However, if everyone chooses the most costly alternative, you will still be better off choosing the most expensive yourself.

Table 1. Benefit distribution based on chosen learning for a self-learning system: cost-effectiveness and maximum of protection.[a]

	Everyone else chooses CEA logic	Everyone else chooses max protection
You choose CEA logic	You: 10; society: 10	You: 6; society: 7
You choose max protection	You: 15; society: 9	You: 7; society: 6

[a]I have here taken 10 as an indicator of a form of status quo, and please note that this is only a thought experiment.

The issue of unexpected or secondary findings are defined as "findings having potential health or reproductive importance for an individual, discovered in the course of conducting a particular study (in research, clinical care or screening) but beyond the aims of that study" [45, p. 248]. Secondary findings is much discussed in genetic screening [46], but it is also a theme in debates over cancer screenings [47]. These findings raise ethical issues since there are perils for false positives, possible impacts on relatives and unlikely net benefits [45], but also economic considerations because both the screening procedures and the possible interventions are costly – and the state of research is often lagging behind the practice of introducing screenings [48].

I propose to look at a smart home technology with possibilities to detect changes in health as a form of constant screening. This assumption might well be challenged, but studies performed with different forms of sensors have among other issues aimed to discover onset of cognitive decline [15, 49], predict increased risks of falls [50], identify heart rate changes and movement changes [51], and the onset of Alzheimer's disease through retina scans [52]. These forms of input into a health decision system could make a real-time prognosis of a person's health status, and that is why I perceive such a future system as continuous screening. It consequently seems probable then that such a system would detect unexpected or secondary findings that raise the issue of novel treatments or interventions where the person is likely to benefit. On the issue of possible future costs, it seems likely that the short-term expenses would increase, but it is difficult to say anything definite about the long-term costs other than that the Presidential Commission for the Study of Bioethical Issues argues for cost-effectiveness to be a central part of future research into incidental findings [53]. If such incidental findings do not constitute a total increased cost, they at least increase the uncertainty concerning any form of screening or diagnostic situation as well as the risks for increased costs.

In Table 2, I have applied the thoughts from Bonnefon et al. to a situation where one could also ask to be given the possibility to be informed about and treated for unexpected findings, in which there is a veritable race to the bottom [44].

This could indicate that the introduction of smart homes as a form of health monitoring technology should consider what types of options are presented and that there is a need for solid integration into the health system from the onset, in order to develop a form of loyalty and trust between the health provider and the prospective users. Otherwise, the total benefits might be significantly less then hoped for.[2]

Related to this issue is the need to maintain a readiness for audits of the different possible institutional logics inherent in AI systems (for health) and in addition a discussion between stakeholders on what form of bias could be inherent in the algorithms' uses. This seems to be called for by the GDPR demand for an explanation of the logic involved in automated decisions regarding health. In the case listed above, one method of conducting audits is through functionality auditing which, "allows for prediction of results from new inputs and explanation of the rationale behind decisions, such as why a new input was assigned a particular classification" [55, p. 4994]. Central to the

[2] From the user perspective, information concerning illnesses where no cure is possible or a continuous deteriorating condition might be stressful and decrease quality of life. See [54].

Table 2. Benefit distribution based on chosen learning for a self-learning system: cost-effectiveness, maximum of protection and action on unexpected findings.

	Everyone else chooses CEA logic	Everyone else chooses max protection	Everyone else chooses unexpected findings & max protection
You choose CEA logic	You: 10; society: 10	You: 6; society: 7	You: 3; society: 4
You choose max protection	You: 15; society: 9	You: 7; society: 6	You: 4; society: 3
You choose unexpected findings & max protection	You: 20: society: 8	You: 8: society: 5	You: 5: society: 2

dialogue between the stakeholders will then be the purpose of the function of the algorithm: is it there to reduce a risk to the company (or any producer of health services) or is its main purpose to reduce individual risk based on personalized risk management parameters?

8 Future Consent

The concept of privacy by default integrated into the GDPR is built upon the double idea of data minimization and purpose specification. Now purpose specification has two dimensions: one relates to the information sought, i.e. how a data collecting system is set up in order to acquire only relevant data for the assigned function; and the other relates to data not being used for any other function which is secondary to the stated purpose for data collection.

Now there is nothing in the case analysis above that is impossible to explain to well-functioning and cognitively alert Oscar, but that raises the issue of who should be responsible for providing and communicating the privacy consequences, the content and the prioritizing logics – as well as possible conflicts between them – to Oscar? What is further at stake here is how these different priorities can be explained to a person who is actually in need of some form of decisional support, but is still competent enough to provide adequate replies to what she or he would prefer to happen in a given situation. From the literature on consent, it seems that if one accepts that informed consent is central to intervention into the private sphere, then it follows that the expert needs to adapt the message to the receiver.

How can one then justify an approach where the security system turns on more privacy breaching surveillance based on large amounts of health data combined with input from medical science if the demand is that "meaningful information about the logic involved" must be explained to Oscar for the system to be allowed to become more invasive? Regardless of how possible, probable, improbable or impossible one sees the example, one issue nevertheless remains: someone (other than Oscar) will in the present and in a possible future be charged with the task of deciding and or implementing levels of privacy for Oscar. For people with declining cognitive

functions, the question of competence for consent is hard to assess. If we assume that the need for safety and security increases with deteriorating cognitive function [56], then there is consequently a challenge in explaining more advanced and new functions to persons with lesser capacity for understanding. In practice, it seems most likely that the phone manufacturer and the data gathering entities as well as the providers of the security system are responsible for talking with Oscar, and they have an incentive to do so since failure to comply could mean economic loss.

When addressing the issue of an advance consent to certain informational privacy agreements, a procedure that is able to maintain the voluntariness of an individual should be seen as ethically preferable to one that does not, since it respects the second criterion, voluntariness, in Beauchamp and Childress' analytics of informed consent [20]. However, as Novitzky et al. point out, this form of consent needs to be maintained in some manner since there might be important contextual factors – internal or external – that can affect the quality of life of an individual in an automated setting [57]. If a formal or informal caregiver suspects or believes that the individual does not any longer benefit from some of the services rendered by a smart home setting, then alternatives should be sought. It is not difficult to imagine a range of scenarios where quality of life decreases due to automated procedures because of lack of perceived agency [33], and these need to be explored systematically [58].

Our suggested approach would be to construct a type of forward-looking consent based on privacy preferences. This type of consent could take as a point of departure Oscar's choices before his health deteriorates – or at the start of a deterioration. One possible point of departure might be to apply analytics drawn from a pragmatic framework for the understanding of privacy, such as the one developed by Daniel Solove [35]. Solove's framework is a useful point of departure since it can refer to types of privacy and types of privacy violations. However, the specific circumstances that should or should not count as adequate, sufficient and necessary grounds for breaching any type of person's privacy are left out. This might be the space for ethics. There are some approaches in the literature to which I now will turn my attention.

8.1 Rolling Consent

A central procedure in working with persons with some form of impaired capacity to consent or with persons that a health professional believes might deteriorate below the threshold for consenting, is the so called "rolling informed consent" which consists of (a) providing repeated and unsolicited information on several occasions — and asking consent each time; (b) assessing the speech of the person in order to consider if they still can be said to participate with competence, understanding and voluntariness; and (c) telling the patient that he or she can opt out every time [57]. However, this procedure presupposes that there is a health professional (or researcher) present who might give precise information about the situation. In Oscar's situation above, this might be the case, but it might also not be the case. Furthermore, since we are talking here about increased surveillance and possible intrusion, it is not clear whether a health professional will have the necessary knowledge of the processing of the information against other types of data and the possible consequences for Oscar in case of a breach.

A change in the current professional education and practice – or even a form of specialization – would be needed to remediate this current lack of knowledge.

8.2 Automated Privacy Settings

There have been several suggestions for automated privacy settings. Here I will discuss two, which I see as promising but not entirely ideal for the case at hand. Michelle Thorne and Peter Bihr suggest developing a privacy keyfob, a small hardware device with built-in authentication mechanisms, which can tell its user or wearer what the privacy settings are of any new surveillance or smart house system [59]. The keyfob user can then choose to enter or take adequate precautions, such as not disclosing information thought to be in some way sensitive. Such a keyfob could also be used in the opposite direction, i.e. to instruct the surveillance or smart house system. Florian Schaub et al. propose a system for "in situ privacy decision support" [60]. Their approach is based on a range of sensors that give signals when there are occurrences that ought not to happen in a given context. The system is divided into three connected models: a context model; a privacy decision engine; and realization and enforcement. These models are divided into a system level and a decision level. For the context model, the system level consists of context information necessary to make decisions, and the decision level consists of a user and its surroundings and activities. These create an environment, or a context. In the privacy decision engine, detected changes in context lead to a consideration of privacy relevance. The privacy settings have been created through case input, and there is an adaptive learning from experience in the program. In the realization and enforcement model, privacy policies are determined according to private or public area and further to the degree of identification of the individual depending on the place.

Both these approaches could well be part of different future privacy arrangements. However, they seem to lack procedures in their current setup for changes in medical conditions and perceived values of new trade-offs for people with potentially diminished capacity to consent.

Since the different future dimensions of privacy that might be affected are also related to health, one suggestion would be that the discussion with Oscar about his future privacy arrangements take place in cooperation with a health professional in order to increase health benefits and avoid different forms of interrogations by data collecting entities that are irrelevant for Oscar's welfare. Based on central insight from, for example, occupational therapy, it is feasible to document which functions people value receiving and performing themselves [61]. Such documentation of functions might well then be the basis for a discussion on what data will be gathered, processed, shared and used as a basis for supporting Oscar. For a smart function to be based on information about a person, then it is necessary that this function is important to the person in question: if I do not really care much to know more about my deteriorating COPD, then increased monitoring seems of little value to me. The importance of a possibility to change privacy settings in dialogue with the users is also proposed by Ella Kolkowska [62]. The dialogue with the users depends on a suitable model for interaction between users (patients) and professionals (medical personnel). Ezekiel J. and Linda I. Emanuel present a modified form of a deliberative model for physician-patient

interaction [63]. Here "the patient is empowered not simply to follow unexamined preferences or examined values, but to consider, through dialogue, alternative health-related values, their worthiness, and their implications for treatment" [63, p. 247]. In this regime, as with the "rolling consent", the main issue would be to educate health professionals as to the possible consequences of different sorts of improper informational privacy breaches, as expressed by Solove [35].

9 Conclusion

I have presented some dilemmas that might occur with the smart solutions for increased home residency among older adults. Of course, there might also be other dilemmas [14]. On one level, I have not showed more than a need for professional, as well as larger societal involvement in the processes, where an emphasis on health and safety would yield one desirable action or sets of action and a focus on privacy would problematize those actions. On another level, the arguments above point towards a possible reconfiguration of informed consent since "artificial intelligences often excel by developing whole new ways of seeing, or even thinking, that are inscrutable to us" [64]. Such changes point towards a conflict with the GDPR, but if the results provided were valuable, then it would be unethical to rule them out a priori because of a lack of understanding of the mechanisms behind the results. The concept and the practice of informed consent has been in development and will continue to develop [65].

From a different perspective, I have touched upon the theme of future costs connected to people's ability to choose for themselves. If we, as societies, wish to keep the same level of health services with the same amount of costs, then it seems that the choices provided with smart solutions need to be limited if the aim is to maximize utility. In this situation as well, there is a both a normative and an epistemic challenge in obtaining consent [66, 67].

Any solution to such dilemmas seems to require some degree of participation by health professionals which again presupposes that they have the knowledge to be a part of such solutions.

Acknowledgments. The project, 'The Assisted Living Project: Responsible innovations for dignified lives at home for persons with mild cognitive impairment or dementia', is financed by the Research Council of Norway under the SAMANSVAR strand (247620/O70). I have presented parts of the thoughts discussed here at *Ethics and Artificial Intelligence* in Kristiansand, December 4–5, 2017. Thanks to Einar Duenger Bøhn for organizing the event and all participants for valuable input. I am very grateful to all the persons who have dedicated time to the Assisted Living project, and I thank the reviewers for valuable questions and suggestions as well as Marie Sjölinder for the invitation to submit the current article.

References

1. Forsberg, E.-M., Thorstensen, E.: A Report from the field: doing RRI from scratch in an assisted living technology research and development project. In: Ferri, F., Dwyer, N., Raicevich, S., Grifoni, P., Altiok, H., Andersen, H.T., Laouris, Y., Silvestri, C. (eds.) Governance and Sustainability of Responsible Research and Innovation Processes, pp. 19–26. Springer International Publishing, Cham (2018). https://doi.org/10.1007/978-3-319-73105-6_3
2. Selbst, A.D., Powles, J.: Meaningful information and the right to explanation. Int. Data Priv. Law **7**, 233–242 (2017)
3. Goodman, B., Flaxman, S.: EU regulations on algorithmic decision-making and a "right to explanation". In: International Machine Learning, pp. 1–6 (2016)
4. Wachter, S., Mittelstadt, B., Floridi, L.: Why a right to explanation of automated decision-making does not exist in the general data protection regulation. Int. Data Priv. Law **7**, 76–99 (2017)
5. von Schomberg, R.: A vision of responsible research and innovation. In: Owen, R., Bessant, J., Heintz, M. (eds.) Responsible Innovation: Managing the Responsible Emergence of Science and Innovation in Society, pp. 51–74. Wiley, Chichester (2013)
6. Macnaghten, P.: The Metis of Responsible Innovation: Helping Society to Get Better at the Conversation Between Today and Tomorrow. Wageningen University, Wageningen (2016)
7. Coenen, C.: Deliberating visions: the case of human enhancement in the discourse on nanotechnology and convergence. In: Kaiser, M., Kurath, M., Maasen, S., Rehmann-Sutter, C. (eds.) Governing Future Technologies, pp. 73–87. Springer, Netherlands (2010). https://doi.org/10.1007/978-90-481-2834-1_5
8. Owen, R., Stilgoe, J., Macnaghten, P., Gorman, M., Fisher, E., Guston, D.: A framework for responsible innovation. In: Owen, R., Bessant, J., Heintz, M. (eds.) Responsible Innovation, pp. 27–50. Wiley, Chichester (2013)
9. Scherer, M.J.: The change in emphasis from people to person: introduction to the special issue on assistive technology. Disabil. Rehabil. **24**, 1–4 (2002)
10. Balta-Ozkan, N., Davidson, R., Bicket, M., Whitmarsh, L.: The development of smart homes market in the UK. Energy **60**, 361–372 (2013)
11. Thygesen, H.: Technology and good dementia care. A study of technology and ethics in everyday care practice. Centre for Technology, Innovation and Culture (TIK), University of Oslo, Oslo (2009)
12. Sturm, J.: Persuasive technology. In: van Hoof, J., Demiris, G., Wouters, Eveline J.M. (eds.) Handbook of Smart Homes, Health Care and Well-Being, pp. 3–12. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-01583-5_56
13. Thorstensen, E.: Responsible help at home: establishing indicators for a product assessment methodology. In: Bowman, D.M., Dijkstra, A.M., Fautz, C., Guivant, J., Konrad, K., Shelley-Egan, C., Woll, S. (eds.) The Politics and Situatedness of Emerging Technologies. IOS Press, Berlin (2017)
14. Sánchez, V.G., Taylor, I., Bing-Jonsson, P.C.: Ethics of smart house welfare technology for older adults. Int. J. Technol. Assess. Health Care **3**, 691–699 (2017)
15. Nijhof, N., Van Gemert-Pijnen, L.J., Woolrych, R., Sixsmith, A.: An evaluation of preventive sensor technology for dementia care. J. Telemed. Telecare **19**, 95–100 (2013)
16. Peek, S.T.M., Aarts, S., Wouters, E.J.M.: Can smart home technology deliver on the promise of independent living? In: van Hoof, J., Demiris, G., Wouters, E.J.M. (eds.) Handbook of Smart Homes, Health Care and Well-Being, pp. 1–10. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-01904-8_41-2

17. Li, K.F.: Smart home technology for telemedicine and emergency management. J. Ambient Intell. Hum. Comput. **4**, 535–546 (2013)
18. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016). L 119, pp. 1–88. Official Journal of the European Union Volum 59
19. van Dijk, N., Gellert, R., Rommetveit, K.: A risk to a right? Beyond data protection risk assessments. Comput. Law Secur. Rev. **32**, 286–306 (2016)
20. Beauchamp, T.L., Childress, J.F.: Principles of Biomedical Ethics. Oxford University Press, New York (2013)
21. O'Neill, O.: Some limits of informed consent. J. Med. Ethics **29**, 4–7 (2003)
22. Turkle, S.: Alone Together: Why We Expect More from Technology and Less from Each Other. Basic Books, New York (2012)
23. Coeckelbergh, M.: Robot rights? Towards a social-relational justification of moral consideration. Ethics Inf. Technol. **12**, 209–221 (2010)
24. Gerdes, A.: The issue of moral consideration in robot ethics. SIGCAS Comput. Soc. **45**, 274–279 (2016)
25. Diakopoulos, N.: Algorithmic Accountability Reporting: On the Investigation of Black Boxes. Tow Center for Digital Journalism (2013)
26. Pasquale, F.: The Black Box Society: The Secret Algorithms that Control Money and Information. Harvard University Press, Cambridge (2015)
27. Ben-Shahar, O., Schneider, C.: More Than You Wanted to Know: The Failure of Mandated Disclosure. Princeton University Press, Princeton (2014)
28. Topo, P.: Technology studies to meet the needs of people with dementia and their caregivers: a literature review. J. Appl. Gerontol. **28**, 5–37 (2008)
29. Wynne, B.: Creating public alienation: expert cultures of risk and ethics on GMOs. Sci. Cult. **10**, 445–481 (2001)
30. Davies, S.R., Macnaghten, P.: Narratives of mastery and resistance: lay ethics of nanotechnology. Nanoethics **4**, 141–151 (2010)
31. Brunsting, S., Best-Waldhober, M.D., Feenstra, C.F.J., Mikunda, T.: Stakeholder participation practices and onshore CCS: lessons from the Dutch CCS case Barendrecht. Energy Procedia **4**, 6376–6383 (2011)
32. Dignum, M., Correljé, A., Cuppen, E., Pesch, U., Taebi, B.: Contested technologies and design for values: the case of shale gas. Sci. Eng. Ethics **22**, 1171–1191 (2016)
33. Hofmann, B.: Ethical challenges with welfare technology: a review of the literature. Sci. Eng. Ethics **19**, 389–406 (2013)
34. Barocas, S.: Data mining and the discourse on discrimination. In: Data Ethics Workshop, Conference on Knowledge Discovery and Data Mining (2014)
35. Solove, D.: A taxonomy of privacy. Univ. Pennsylvania Law Rev. **154**, 477–560 (2006)
36. Solove, D.: Conceptualizing privacy. California Law Rev. **90**, 1087 (2002)
37. Nordmann, A.: If and then: a critique of speculative nanoethics. Nanoethics **1**, 31–46 (2007)
38. Stahl, B.C., McBride, N., Wakunuma, K., Flick, C.: The empathic care robot: a prototype of responsible research and innovation. Technol. Forecast. Soc. Change **84**, 74–85 (2014)
39. Washington, N., Kelly, D.: Who's responsible for this? Moral responsibility, externalism, and knowledge about implicit bias. In: Brownstein, M., Saul, J.M. (eds.) Implicit Bias and Philosophy. Volume 2, Moral Responsibility, Structural Injustice, and Ethics, pp. 11–36 (2016)
40. McDonald, A.M., Cranor, L.F.: The cost of reading privacy policies. I/S J. Law Policy Inform. Soc. **4**, 540–565 (2008)

41. Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L.F., Komanduri, S., Leon, P.G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., Wilson, S.: Nudges for privacy and security: understanding and assisting users' choices online. ACM Comput. Surv. **50**, 44:41–44:41 (2017)
42. Faber, P.: Client and professional. In: Rowan, J.R., Zinaich, S. (eds.) Ethics for the Professions, pp. 125–134. Wadsworth Thomson Learning, Belmont (2002)
43. Russell, S.J., Norvig, P., Davis, E.: Artificial Intelligence: A Modern Approach. Prentice Hall, Upper Saddle River (2010)
44. Bonnefon, J.-F., Shariff, A., Rahwan, I.: The social dilemma of autonomous vehicles. Science **352**, 1573–1576 (2016)
45. Christenhusz, G.M., Devriendt, K., Dierickx, K.: To tell or not to tell? A systematic review of ethical reflections on incidental findings arising in genetics contexts. Eur. J. Hum. Genet. **21**, 248–255 (2013)
46. Mackley, M.P., Capps, B.: Expect the unexpected: screening for secondary findings in clinical genomics research. Br. Med. Bull. **122**, 109–122 (2017)
47. Hofmann, B.: Ethical issues with colorectal cancer screening—a systematic review. J. Eval. Clin. Pract. **23**, 631–641 (2017)
48. Douglas, M.P., Ladabaum, U., Pletcher, M.J., Marshall, D.A., Phillips, K.A.: Economic evidence on identifying clinically actionable findings with whole-genome sequencing: a scoping review. Genet. Med. **18**, 111–116 (2016)
49. Hayes, T.L., Abendroth, F., Adami, A., Pavel, M., Zitzelberger, T.A., Kaye, J.A.: Unobtrusive assessment of activity patterns associated with mild cognitive impairment. Alzheimer's Dement. **4**, 395–405 (2008)
50. Stone, E.E., Skubic, M.: Fall detection in homes of older adults using the Microsoft kinect. IEEE J. Biomed. Health Inform. **19**, 290–301 (2015)
51. Spenko, M., Yu, H., Dubowsky, S.: Robotic personal aids for mobility and monitoring for the elderly. IEEE Trans. Neural Syst. Rehabil. Eng. **14**, 344–351 (2006)
52. Koronyo, Y., Biggs, D., Barron, E., Boyer, D.S., Pearlman, J.A., Au, W.J., Kile, S.J., Blanco, A., Fuchs, D.-T., Ashfaq, A., Frautschy, S., Cole, G.M., Miller, C.A., Hinton, D.R., Verdooner, S.R., Black, K.L., Koronyo-Hamaoui, M.: Retinal amyloid pathology and proof-of-concept imaging trial in Alzheimer's disease. JCI Insight **2**, 93621 (2017)
53. The Presidential Commission for the Study of Bioethical Issues: Anticipate and Communicate: Ethical Management of Incidental and Secondary Findings in the Clinical, Research, and Direct-to-Consumer Contexts. CreateSpace Independent Publishing Platform (2015)
54. Hansen, L.A., Almqvist, F., Ørjasæter, N.-O., Kistorp, K.M.: Velferdsteknologi i sentrum (VIS) - evaluering av velferdsteknologi fra et tjenestedesignperspektiv. Tidsskrift for omsorgsforskning **3**, 144–152 (2017)
55. Mittelstadt, B.: Automation, algorithms, and politics| Auditing for transparency in content personalization systems. Int. J. Commun. **10**, 12 (2016)
56. de Maagt, S., Robeyns, I.: Can person-centered care deal with atypical persons? Am. J. Bioeth. **13**, 44–46 (2013)
57. Novitzky, P., Smeaton, A.F., Chen, C., Irving, K., Jacquemard, T., O'Brolcháin, F., O'Mathúna, D., Gordijn, B.: A review of contemporary work on the ethics of ambient assisted living technologies for people with dementia. Sci. Eng. Ethics **21**, 707–765 (2015)
58. Cavoukian, A., Mihailidis, A., Boger, J.: Sensors and in-home collection of health data: a privacy by design approach. Information and Privacy Commissioner of Ontario (2010)
59. Thorne, M., Bihr, P.: Understanding the connected home: thoughts on living in tomorrow's connected home, 2nd edn. (2016). https://legacy.gitbook.com/download/pdf/book/connected-home-book/understanding-the-connected-home. Accessed 12 Jan 2018

60. Schaub, F., Könings, B., Weber, M., Kargl, F.: Towards context adaptive privacy decisions in ubiquitous computing. In: 2012 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), pp. 407–410 (2012)
61. Law, M., Baptiste, S., McColl, M., Opzoomer, A., Polatajko, H., Pollock, N.: The Canadian occupational performance measure: an outcome measure for occupational therapy. Can. J. Occup. Ther. **57**, 82–87 (1990)
62. Kolkowska, E.: Privacy principles in design of smart homes systems in elderly care. In: Tryfonas, T., Askoxylakis, I. (eds.) HAS 2015. LNCS, vol. 9190, pp. 526–537. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-20376-8_47
63. Emanuel, E.J., Emanuel, L.l.: Four models of the physician-patient relationship. In: Rowan, J.R., Zinaich, S. (eds.) Ethics for the Professions, pp. 245–254. Wadsworth Thomson Learning, Belmont (2002)
64. Kuang, C.: Can A.I. Be Taught to Explain Itself? The New York Times (2017)
65. Veatch, R.M.: Abandoning informed consent. Hastings Cent. Rep. **25**, 5–12 (1995)
66. Cohen, S.: Nudging and informed consent. Am. J. Bioeth. **13**, 3–11 (2013)
67. Ploug, T., Holm, S.: Doctors, patients, and nudging in the clinical context-four views on nudging and informed consent. Am. J. Bioeth. AJOB **15**, 28–38 (2015)