Ethics Inf Technol
DOI 10.1007/s10676-017-9426-4

ORIGINAL PAPER

Ethics of the health-related internet of things: a narrative review

Brent Mittelstadt[1,2,3]

Abstract The internet of things is increasingly spreading into the domain of medical and social care. Internet-enabled devices for monitoring and managing the health and well-being of users outside of traditional medical institutions have rapidly become common tools to support healthcare. Health-related internet of things (H-IoT) technologies increasingly play a key role in health management, for purposes including disease prevention, real-time tele-monitoring of patient's functions, testing of treatments, fitness and well-being monitoring, medication dispensation, and health research data collection. H-IoT promises many benefits for health and healthcare. However, it also raises a host of ethical problems stemming from the inherent risks of Internet enabled devices, the sensitivity of health-related data, and their impact on the delivery of healthcare. This paper maps the main ethical problems that have been identified by the relevant literature and identifies key themes in the on-going debate on ethical problems concerning H-IoT.

Keywords Internet of things · Data ethics · Medicine · Data analytics · Privacy · Review

✉ Brent Mittelstadt
bmittelstadt@turing.ac.uk

[1] Oxford Internet Institute, University of Oxford, 1 St Giles, Oxford OX1 3JS, UK

[2] The Alan Turing Institute, British Library, 96 Euston Rd, London NW1 2DB, UK

[3] Department of Science and Technology Studies, University College London, 22 Gordon Square, London WC1E 6BT, UK

Introduction

The internet of things is increasingly spreading into the domain of medical and social care. Internet-enabled devices for monitoring and managing the health and well-being of users outside of traditional medical institutions have rapidly become common tools to support healthcare. Health-related internet of things (H-IoT) technologies increasingly play a key role in health management, for purposes including disease prevention, real-time tele-monitoring of patients functions, testing of treatments, fitness and well-being monitoring, medication dispensation, and health research data collection (Empirica 2010; Schmidt and Verweij 2013). At the same time, many preventative and clinical applications exist, from proactive self-monitoring of fitness and well-being (e.g. sleep quality, activity levels) to 'smart home' assistive devices that assist in 'ageing at home'. Devices range from single-sensor mobile devices to complex spatial networks capable of measuring health (e.g. physiological parameters) and health-related behaviours (e.g. sleep, ambulation) for external- and self-management of health and well-being. In the same vain, apps and software updates can similarly transform existing networked devices into H-IoT.[1] Tens of thousands of such health-related apps are now available for consumption (Lupton 2015).

The applications of H-IoT are wide, including clinical, consumer, and research applications. H-IoT can be used for many purposes, including long-term monitoring and

[1] Examples include the Health app for pebble smart watches, Health2Sync or one drop for glucose monitors and smart phones, or ResearchKit and Google Fit for iOS and Android devices, respectively.

Published online: 04 July 2017

management of health and chronic illness, and consumer-level health and well-being management.[2] At-risk patients can be monitored for health emergencies or conditions, replacing time-consuming activities such as home nursing observations (E-Health Insider 2014). Chronic conditions often require long stays in hospital or hospitalization at short notice, the use of H-IoT may help patients to stay at home and live a more normal life (Empirica 2010; Remmers 2010; van Hoof et al. 2011) and to reduce costs and hospitalization rates (Henderson et al. 2013; Lomas 2009).

H-IoT can monitor parameters such as heart rate, respiration, blood oxygen saturation, skin temperature, blood glucose, blood chemistry, and body weight can be collected alongside behavioural parameters (e.g. motion, acceleration, mood) linked to health and well-being. The health and behaviours of users can be digitised, recorded, stored, and analysed, creating novel opportunities for clinical care and research, including alerts and medication dispensing by devices (Lupton 2014a). H-IoT analytics protocols, in turn, use these data to generate information about different aspects of the user's health including emergencies (e.g. heart attacks) or health-related behaviour (e.g. exercise, sleep). Data streams from multiple sensors can be aggregated to facilitate linked-up care and health management. Novel connections can be found between areas of private life traditionally outside the scope of health and healthcare (Bowes et al. 2012).

Data produced by H-IoT create opportunities to advance the diagnosis, treatment, and prevention of diseases, and to foster healthy habits and practices (Costa 2014) among individual users and broader populations (e.g. patient cohorts). These data may also further the understanding of the contributing factors to disease and the efficiency and effectiveness of treatments and health organisations. Realising these opportunities requires responsible and permissive design of H-IoT data collection, analysis, and sharing protocols. Linking H-IoT data with other biomedical datasets, including aggregated clinical trials (Costa 2014), genetic and microbiomic sequencing data (The NIH HMP Working Group et al. 2009; Mathaiyan et al. 2013; McGuire et al. 2008), scraped and publicly accessible internet data (Lupton 2014b, p. 858; Costa 2014), biological specimens, electronic health records and administrative hospital data can allow for novels insights between traditional medical care and at-home behaviours.[3] H-IoT can be conceived of as a component of biomedical 'Big Data' (Mittelstadt and Floridi 2016) when the generated data are linked to other medical datasets.

As these examples show, H-IoT presents many possible benefits for patient health and healthcare, and may play a key role in meeting potential shortfalls in healthcare attributed to ageing demographics (United Nations 2008; Population Reference Bureau 2012). One of the main challenges of H-IoT is how to design devices and protocols to collect, share, process, and validate data across different application domains in ways that are economically efficient, technologically robust, scientifically reliable, and ethically sound.

H-IoT raises a host of ethical problems stemming from the inherent risks of Internet enabled *devices*, the sensitivity of health-related *data*, and their impact on the delivery of *healthcare*. A primary challenge of H-IoT is to ensure that devices and protocols for sharing the data that they create are technologically robust and scientifically reliable, while also remaining ethically responsible, trustworthy, and respectful of user rights and interests.

Privacy is also critical, as H-IoT devices can create a personal health and activity record of unprecedented scope and granularity. Once data have been generated by a device, they must be transmitted, curated, labelled, stored, and analysed for the benefit of the user, service provider, and other stakeholders. Protocols for each of these steps can similarly be designed in more or less ethically acceptable ways. A protocol that, for instance, retains data indefinitely without a clearly defined purpose may be more worrisome than storage with well-defined limitations, scope, and purpose. The role of the user (or data subject) in subsequent processing and control of data generated by H-IoT must be considered on ethical as well as legal grounds.

Ethical assessment is a key component for the adoption of new medical technologies. This paper provides a narrative overview of academic discourse, identifying three key themes in discussion of ethical issues concerning H-IoT, which we call the ethics of devices, data, and practices. "Methodology" section describes the narrative review methodology. "Ethical issues for H-IoT devices" through "Ethical issues for H-IoT mediated care" sections review ethical issues in H-IoT from device, data, and practice perspectives. "Conclusion" section concludes with reflections on future research.

[2] Terminological overlap exists between H-IoT and similar technologies including health applications of ubiquitous computing and ambient intelligence (Bohn et al. 2005; Brey 2005), assistive technologies (Zwijsen et al. 2011), telecare, telehealth and telemedicine (Stowe and Harding 2010).

[3] In some contexts, such as the USA under HIPAA, administrative data will be afforded less protection than genomic and similar biobank data despite possessing similar capacities for revealing sensitive aspects of a person's health. This may be due partly to the possibility of removing identifiers from administrative data without 'ruining' the data (Currie 2013) as is an apparent limitation with anonymisation of genomic data (Hansson 2009).

Table 1 Database search queries and results

Database	Search query	Returned
Web of science	**TOPIC**: (ethic* OR moral*) *AND* **TOPIC**: ("internet of things" OR "IoT" OR "ubiquitous computing" OR "ambient intelligence" OR "smart homes" OR wearable* OR "big data" OR "health monitoring") *AND* **TOPIC**: (health* OR medic* OR bio*)	192
Scopus	**TITLE-ABS-KEY** (ethic* OR moral*) **AND TITLE-ABS-KEY** ("internet of things" OR "IoT" OR "ubiquitous computing" OR "ambient intelligence" OR "smart homes" OR wearable* OR "big data" OR "health monitoring") **AND TITLE-ABS-**KEY (health* OR medic* OR bio*)	332
Global health	(ethic* OR moral*) AND ("internet of things" OR "IoT" OR "ubiquitous computing" OR "ambient intelligence" OR "smart homes" OR wearable* OR "big data" OR "health monitoring") AND (health* OR medic* OR bio*)	88
Philpapers (complex search queries not supported)	ethic* AND ("internet of things" OR "IoT" OR "big data" OR "health monitoring")	42
PubMed	(ethic* OR moral*) AND ("internet of things" OR "IoT" OR "ubiquitous computing" OR "ambient intelligence" OR "smart homes" OR wearable* OR "big data" OR "health monitoring") AND (health* OR medic* OR bio*)	154
Google scholar	(ethic* OR moral*) AND ("internet of things" OR "IoT" OR "ubiquitous computing" OR "ambient intelligence" OR "smart homes" OR wearable* OR "big data" OR "health monitoring") AND (health* OR medic* OR bio*)	Approx. 14,900 (results 1 to 300 reviewed)

Methodology

In order to understand what ethical issues have already been identified and discussed in the context of H-IoT, a systematic survey of academic literature was conducted in November 2016. Results of the survey are presented as a narrative review of the field. The review is systematic insofar as the search methodology used consistent keywords across multiple databases to identify an initial sample of literature (see: Table 1). However, the results are presented as a thematic narrative, which intentionally does not assess the frequency of themes, theories, and concepts across the sample.

Six databases were searched (Web of Science, Scopus, Global Health, Philpapers, PubMed and Google Scholar) to identify literature discussing ethical aspects of H-IoT. Search terms (with wildcards) were chosen to limit the review to articles addressing ethics, health or medicine, and the internet of things and related technologies (e.g. wearables, smart home technologies). The title and abstract of each returned article was reviewed by the author to determine relevance. Inclusion was based solely on the discussion of ethical issues in the article, with the goal of identifying themes in the literature. Limitations were not placed on the quality or length of the discussion, but rather on the mere presence of ethical concepts and issues. Additional sources were also located through hand-searching and backtracking of citations provided within the reviewed articles.

The search was limited to English language articles. Although most of the reviewed literature consisted of peer-reviewed journal articles, other types of publications including commentaries, working reports, white papers and scientific books were also located. Date restrictions were not imposed at the time of the database review. Despite this, the sample reflects a range of sources from 2000 to 2016. Figure 1 provides a breakdown of sources by year of publication.

A total of 1108 non-unique sources were returned from the six database queries. Titles and in some cases abstracts for each article were assessed for initial sorting. A total of 128 sources were fully reviewed. Each fully reviewed article was analysed, and key passages highlighted for further interpretation and grouping into themes existing across multiple sources. The themes of the debate have therefore been identified *ex post* during the literature analysis rather than a pre-defined thematic framework being used.

After initial assessment of title/abstract combinations to remove off-topic sources, phrases and passages were highlighted that appeared to refer to ethical issues or concepts. Inclusion was thus based on discussion of issues of 'right' and 'wrong', or the clash of competing values or normative interests among stakeholders. Highlighted segments were then coded to reflect the author's interpretation of the text (Gadamer 2004; Patterson and Williams 2002). Finally, similar codes were grouped and assigned to ethical themes.

Once themes had emerged from the literature, a second analysis was run using the NVivo 10 software package. A keyword frequency search was used to identify important concepts or themes that were missed in the first round of hand analysis. Multiple keyword searches based on themes and key phrases that emerged from the initial round of analysis were run across the sample. This approach ensured that the narrative overview reflected all sources discussing

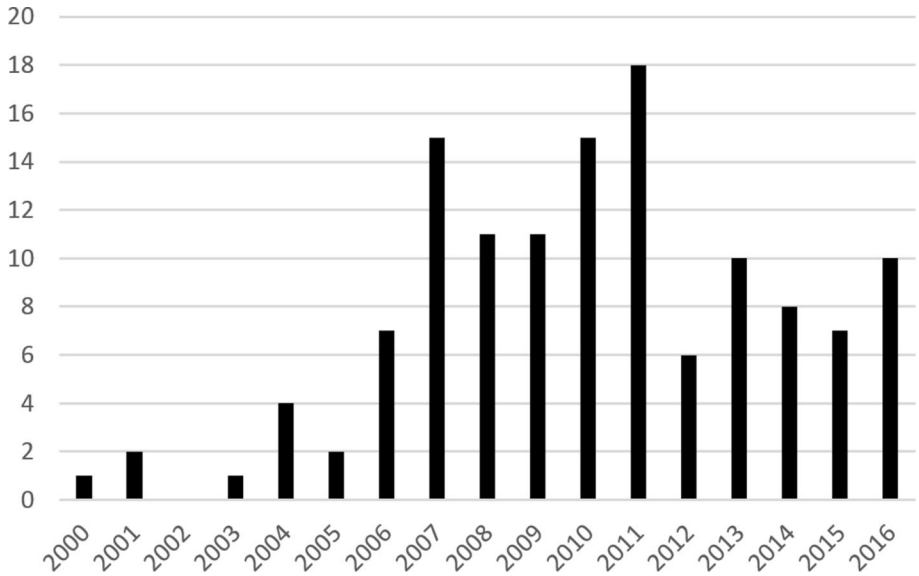

Fig. 1 Sources by year of publication

a theme, and not only those from which the theme in question was initially identified by hand.

Ethical issues for H-IoT devices

Ethical issues with H-IoT can be considered from a number of perspectives, each highlighting related but different concerns. In this article, we address the ethics of H-IoT at a *device, data*, and *practice* level. The following three sections provide a review of ethical issues with H-IoT centred on devices, data collection, analysis and sharing protocols, and the impact of H-IoT on medical and social care. Some overlapping among the three categories is to be expected. Nonetheless, they provide a useful organising structure for future discussion of ethical design and deployment of H-IoT.

Personal privacy

H-IoT is designed to operate in both private and public environments. Devices can be carried by the user or embedded in environments, such as the home, residential care, workplace or public spaces. In each case, a window into private life is created, enabling the collection of data about the user's health and behaviours and the analysis by third parties. The lives of users can be digitised, recorded, and analysed by third parties, creating opportunities for data sharing, mining, and social categorisation (cf. Lyon 2003). These basic functions may improve healthcare through increasingly granular monitoring and personalised interventions (Pasluosta et al. 2015), yet they simultaneously create an opportunity for violating user expectations of personal and informational privacy.

Personal privacy is a multifaceted right. It refers to aspects of privacy not directly related to control of data and includes both physical and social aspects. On the physical side, privacy is determined by the physical accessibility of a person to others, defined by physical borders, such as doors and walls (Bowes et al. 2012; Brey 2005; Essén 2008; Little and Briggs 2009). This can also be interpreted as a right to possess and protect personal space (Kosta et al. 2010), such as a home. Personal privacy can refer to the right to be left alone or not monitored by a third party (cf. Demiris and Hensel 2009; Dorsten et al. 2009; Mittelstadt et al. 2011; Pallapa et al. 2007; Wilkowska et al. 2010). It concerns feelings of intimacy and control over 'private space' (Gaul and Ziefle 2009; Ziefle et al. 2011). Personal privacy can also be understood as a freedom, to "escape being observed or accessed when desired" (Essén 2008, p. 130), implying a social duty to respect the desire for isolation of others. The introduction of H-IoT may cause a gradual loss of personal privacy (Steele et al. 2009), particularly among smart home systems (Coughlin et al. 2007; Demiris 2009; Dorsten et al. 2009). Monitoring technologies can create a psychological disturbance, sometimes called obtrusiveness (Hensel et al. 2006; Nefti et al. 2010), expressed in a feeling of 'being watched'. Perceived violations of personal privacy are often linked to the types of sensors used, with cameras often linked to severe violations (Caine et al. 2006; Leone et al. 2011; Zwijsen et al. 2011; Tiwari et al. 2010; Stowe and Harding 2010; Demiris et al. 2004). On the social side, personal privacy concerns control over social interaction through geographical distance, group membership, and location. It is connected to physical privacy (Bagüés et al. 2007b; Coughlin et al. 2007; Little and Briggs 2009) and can contribute to social isolation.

For H-IoT used in chronic illness management, potential violations of personal privacy can be justified on the basis of 'need' for the technology, derived from safety concerns (Zwijsen et al. 2011; Steele et al. 2009) or the delay of a move to residential care (Townsend et al. 2011; Remmers 2010; Essén 2008; McLean 2011). This type of 'tradeoff' highlights the potential for H-IoT to simultaneously violate and enhance privacy. A tradeoff has been observed between personal privacy and safety, particularly among the mentally impaired patients (Ojasalo et al. 2010; Stowe and Harding 2010; Landau et al. 2010), as well as frail elderly (Melenhorst et al. 2004; Courtney 2008; Courtney et al. 2008; Steele et al. 2009), and chronically ill persons (Salih et al. 2011; Neild et al. 2004). In these contexts, it has been stressed that personal privacy can be both protected by eliminating the need for in-person care (Ojasalo et al. 2010; Essén 2008) and violated by the presence of a monitoring device (Melenhorst et al. 2004; Steele et al. 2009; Salih et al. 2011). The tradeoff between privacy and safety may be seen as a necessary part of aging, with increasing susceptability to health problems (Steele et al. 2009), though this view should not be applied generally to associate aging with reduced expectations of privacy, or to justify increased privacy violating interventions.

Obtrusiveness, stigma and autonomy

The perceived obtrusiveness and visibility of H-IoT devices affects user acceptance and long-term use (Demiris 2009; Demiris and Hensel 2009; De Bleser et al. 2011; Townsend et al. 2011). Obtrusiveness has been defined as "a summary evaluation by a person based on characteristics or effects associated with the technology that are perceived as undesirable and physically and/or psychologically prominent" (Hensel et al. 2006, p. 430). The definition refers to the distinction between physical and mental obtrusiveness, as seen in non-medical ambient intelligence applications (cf. Brey 2005). A sense of obtrusiveness can lead to subversion of a system's functions, for instance by walking around pressure sensors or otherwise disabling the system (Courtney et al. 2007).

The psychological disappearance of H-IoT when used in personal spaces such as homes or residential care can also cause ethical problems (Ebersold and Glass 2016). H-IoT embedded in a home or care environment may be forgotten following extended use (Essén 2008; van Hoof et al. 2011). Sensors 'fading into the background' may make users more comfortable in the home (Courtney 2008) and preserve its interpersonal character and meaning for residents (cf. Roush and Cox 2000). At the same time, the validity of consent is undermined if users forget that monitoring is occurring. Rather than consent being a one-off event, occasional renewals of consent may be necessary to ensure monitoring has not merely been forgotten. This is particularly important for cognitively impaired users unable to grant consent (Kenner 2008; Bowes et al. 2012). These concerns can extend to guests of a monitored individual, which suggests the possibility of inadvertent monitoring (Neild et al. 2004).

The related concept of visibility refers to the degree to which a H-IoT device is noticeable to the user and others, both at home and in public (Robinson et al. 2007; Landau et al. 2010; Essén 2008; van Hoof et al. 2011). Visibility is not equivalent to obtrusiveness. It describes aesthetic aspects of a device, and their impact on the perceptions of users and others. Characteristics affecting visibility included ease of use, size and weight (Landau et al. 2010).

Highly obtrusive or visible H-IoT devices can be ethically problematic insofar as both types of devices disrupt a user's normal behaviour or autonomous decision-making. In residential care, monitoring has been seen to influence resident's behaviour in monitored areas (Essén 2008), suggesting awareness of embedded H-IoT sensors may influence user behaviour. The presense of sensors in homes has similarly been shown to influence resident's behaviour and daily routine (Tiwari et al. 2010). The perception of being watched is often to blame (Essén 2008). Similarly, risk taking among elderly users, which can represent a desire to retain independence at home despite safety risks, has been observed to lessen in the presence of H-IoT (Remmers 2010; Percival and Hanson 2006).

Obtrusive H-IoT can also impact a user's sense of identity, including by exposing the user to stigma (Courtney 2008). Identity concerns a person's concept of who they are, the moral and social beliefs they embrace and how they relate to others. Attached to the person's body or installed in the personal environment, H-IoT can become an extension of the person and an embodiment of the illness or the physical activity being monitored (Courtney 2008). A person's identity is often affected by an illness or concern which becomes part of their identity, e.g. I'm a schizophrenic or I'm a bad sleeper (Edgar 2005). The use of H-IoT may materialise these concerns.

A distinction can be drawn here between consumers using commercial devices (general for fitness or well-being) and patients using clinical devices. Concerns with obtrusiveness are more obviously relevant to clinical devices, to which stigma may be attached (Hensel et al. 2006; Courtney 2008). Consumer fitness and well-being trackers are designed to be observed or at least aesthetically attractive for users and are unlikely to carry a negative stigma. Similarly, devices re-purposed for H-IoT sensing, such as smart phones, need not be noticeable as H-IoT is different from their main functionality and, thus, they are unlikely to rain obtrusiveness or visibility concerns.

Clinical devices can carry stigma due to an association with a disease or health condition. Stigma can influence a user's sense of identity and behaviours. Elderly users in residential care have, for instance, been seen to experience feelings of frailty when devices are publicly visible, insofar as they indicate ill health or a need for monitoring to others (Courtney 2008). Even when devices are not publicly visible (for instance, when they are worn under clothing, implanted or embedded in surroundings), alerts and reporting of abnormal behaviour or emergencies can have a similar effect. Behaviours indicating frailty are often hidden by elderly or infirm users to control how others perceive them (Percival and Hanson 2006). H-IoT can thus erode the ability to manage public identity.

Similar to consumer devices, design can minimise obtrusiveness to protect a user's decision-making autonomy and sense of identity. Aesthetically pleasing or minimally visible devices, (Wu et al. 2012) can reduce such impact. However, this should not be achieved paternalistically; perceptions of obtrusiveness will vary between users, meaning design choice is essential to allow users to choose devices fitting their particular needs and values. Devices can, for instance, include 'plausible deniability' features that allow imprecise or false secondary data (e.g. location) to be entered by the user (Greenfield 2008; Bagüés et al. 2007a). A balance sensitive to the needs of specific user groups should nonetheless be struck; the inclusion of such a feature on devices designed for cognitively impaired users could, for example, pose a significant safety risk.

Community-wide implementation that ensures a 'level playing field' between residents is another possible solution (Courtney 2008). The ethical acceptability of the latter solution must, however, be questioned, as it violates the norm that H-IoT should only be used as needed, based on the particular situation of an individual (Mittelstadt et al. 2014) "monitoring for monitoring's sake" (Bowes et al. 2012), or pursuing monitoring as an end in itself (Coughlin et al. 2007; McLean 2011) is to be avoided.

Ethical issues for H-IoT data protocols

H-IoT devices generate a large volume and variety of data describing the personal health and behaviours of users. Much of these data can be used for medical research and consumer analytics. The design of protocols to enable user and third party access to H-IoT datasets also raises ethical concerns.

Informational privacy

Informational privacy concerns control of data about oneself (e.g. Chan et al. 2009; Demiris 2009; Jea et al. 2008; Mitseva et al. 2008; Mittelstadt et al. 2011; Tentori et al. 2006; Tiwari et al. 2010; van De; Garde-Perik et al. 2006; van Hoof et al. 2007). At its narrowest, informational privacy can be equated with hiding personally identifiable data from unauthorised parties (Garcia-Morchon et al. 2011; Ahamed et al. 2007), and can be quantifiable (Srinivasan et al. 2008). As health data are normally considered as particularly sensitive both in an ethical and legal sense (Baldini et al. 2016), informational privacy is a central concern for the design and deployment of H-IoT, insofar as it contributes to gain control over the spread of information about the user's health status and history.

Concerns over data control are common in research assessing the privacy experiences of H-IoT users (Coughlin et al. 2007; Courtney 2008; Little and Briggs 2009; Melenhorst et al. 2004; Wilkowska et al. 2010; Henze et al. 2016). Expectations of control must adapt to "a world of numerous interconnected machines constantly talking to each other and observing the real-world environment." User's privacy and decisional autonomy are challenged by the ability of H-IoT "to transfer decisions that impact an individual's life to devices and algorithms and take action on those decisions without the awareness of the individual" (Ebersold and Glass 2016, p. 147).

Local anonymisation of data prior to communication may help prevent unauthorised access or identification of the user (Agrafioti et al. 2011; Clarke and Steele 2015). Similarly, allowing users to enforce privacy preferences before transmitting sensitive data can help protect context-specific expectations of privacy (Baldini et al. 2016; Henze et al. 2016). However, risks of re-identification of anonymised data through aggregation and re-purposing, and the tradeoff between the scientific or commercial value of data and de-identification must be taken seriously (Peppet 2014; Ebersold and Glass 2016; Jiya 2016; Baldini et al. 2016). For both identifiable and de-identified data, policies restricting access to identifiable data (Subramaniam et al. 2010; Bagüés et al. 2007b; Garcia-Morchon et al. 2011) only for acceptable purposes (Massacci et al. 2009; Chakraborty et al. 2011; Beaudin et al. 2006) can address privacy risks. For instance, access can be agreed upon ahead of time for researchers depending on the study to be developed (Master et al. 2014). At the same time, for instance, a user may allow differential access, permitting her data to be used for public health surveillance but not genomics. The transparency of relationships between data collected and purposes of collection is considered to be central to protecting privacy of users (Giannotti and Saygin 2010), who make decisions regarding acceptable uses.

Users may not be aware of the extent to which data can be accessed outside of the context in which they are created (boyd and Crawford 2012), particularly when 'scraped' from publicly accessible Internet platforms. A

helpful distinction has been recognised by boyd and Crawford (2012) between 'being in public', in the sense that many forms of communication on the Internet (e.g. Twitter, forums) are publicly visible by default, and 'being public', or purposefully making something publicly known or accessible. Re-enforcing this distinction in the design of devices may help users form realistic privacy norms for H-IoT. 'Offline' privacy barriers, such as physical walls, can for example be replicated when considering access to data by requiring explicit action by users in order to upload or share data to publicly accessible locations (Mittelstadt and Floridi 2016).

Examples from the literature show that informational and personal privacy can overlap. Data transmission can, for instance, violate both information and physical privacy (Brey 2005; Friedewald et al. 2007). The transmission of personal data by H-IoT devices can transgress privacy protecting natural, social, spatial, temporal, ephemeral, and transitory borders (cf. Marx 2001). At the same time, by controlling the dissemination of personal information, a person may be spared future physical, social, and decisional disturbance from third parties, such as friends, family, and service providers (cf. Friedewald et al. 2007).

Despite the empowerment of users derived from informational privacy, control can justifiably be limited in certain situations. Empirical studies into attitudes towards H-IoT reveal a preference to forego informational privacy in emergency situations (Rashid et al. 2007, p. 191; Steele et al. 2009), which highlights the need to find a balance between the desire to control data and enjoying the benefits of services which require that data. A similar balance is expressed in preferences towards H-IoT for data gathering over human intrusion into the home (cf. Essén 2008). User-end policies have been proposed as a solution which allows users to pre-define a customized level of privacy meeting their expectations (Friedewald et al. 2007; Massacci et al. 2009; Garcia-Morchon et al. 2011). Privacy tools such as these are meant to enable users to freely move between and interact with a range of H-IoT systems without negotiating individual privacy agreements, while respecting the necessity of informed consent (cf. Bagüés et al. 2007b).

The security of H-IoT devices and protocols is a prerequisite for informational privacy and patient safety. In reference to security of data, 'security' and 'privacy' are often used interchangeably (e.g. Ahamed et al. 2007a; Armac et al. 2009; Busnel and Giroux 2010; Chan et al. 2008; Dhukaram et al. 2011; Elkhodr et al. 2011; Garcia-Morchon et al. 2009; Mana et al. 2011; Stuart et al. 2008; Wang et al. 2008). The concepts must be differentiated by their ends: security is concerned with guaranteeing the *quality* of the data collected by and passing through a system in terms of "confidentiality, integrity and availability" (Giannotti and Saygin 2010, p. 75), enabling users to protect *privacy* by controlling dissemination of their data and preventing hacks or breaches (Peppet 2014).

In reference to patient safety, concerns with the vulnerability of devices and protocols to external attacks, breaches, and leaks of data are relevant. Actuating functions are particularly important from a safety perspective, insofar as a breach can seriously compromise the user's health.[4] One can imagine the harm following from a breached automated insulin pump, administrating the wrong dosage to the patient.

Breaches of H-IoT devices that could undermine users' safety would also mine users' trust in the technology, the producers, and the data controller (Sajid and Abbas 2016). Many existing H-IoT 'apps' lack robust privacy practices and policies, and thus fail to comply with data protection accreditation programmes intended to foster trust and protect user privacy (Huckvale et al. 2015). Trust is a prerequisite for H-IoT systems to be viewed as privacy enhancing in the context of informational privacy (Bagüés et al. 2010; Chakraborty et al. 2011; Coughlin et al. 2009; Dhukaram et al. 2011; Rashid et al. 2007; Wang et al. 2008; Yuan et al. 2007). In this case, trust involves the system collecting and processing data, users providing the data, and stakeholders accessing the data (Bagüés et al. 2010, p. 352; Little and Briggs 2009; Kosta et al. 2010; Taddeo 2010a; Taddeo and Floridi 2011). Lack of trust has been linked to reluctance among potential users to use a give technology and can, thus, undermine adoption of H-IoT (McLean 2011; Brey 2005).

Trust can be understood as a combination of the credibility, motivation, transparency, and responsibility of a system, understood as a combination of devices, developers, data controllers, and users. Credibility is linked to reputation (Little and Briggs 2009; Rashid et al. 2007, p. 190; Taddeo 2010b), insofar as a data controller must be seen as responsible or credible enough to handle sensitive personal data. Motivation refers to the intentions of stakeholders, or how they intend to use the data of users. Monitoring of parameters or putting data to uses beyond those explicitly agreed upon by users can undermine trust. These motivations, and intended uses of data, should be transparent to users, as should the sum of data collected and held about them. To achieve trust, systems must allow

[4] Although very relevant to ethical assessment, a full review of security issues with H-IoT goes beyond the scope of this paper. For further discussion, see: Elkhodr et al. (2011), Garcia-Morchon et al. (2011), Busnel and Giroux (2010), Stuart et al. (2008), Center for Devices and Radiological Health (2014), Peppet (2014). The same comments apply to the issue of standardization, which is key for the security and interoperability of devices and protocols, and thus for data privacy and portability. For further discussion, see Bandyopadhyay and Sen (2011), Greenfield (2008).

users to review and control their data (see also "Data sharing and autonomy" and "Ownership and data access" sections).

Data sharing and autonomy

Autonomy can refer to a right to make personal decisions (Demiris 2009), a right to freedom (Brey 2005), or a right to independence (Remmers 2010). Autonomy is often discussed in terms of freedom and independence, particularly in reference to assistive technologies (Remmers 2010; Zwijsen et al. 2011; Robinson et al. 2007), smart homes (Remmers 2010; Townsend et al. 2011; Brey 2005), and H-IoT embedded in residential care (Dorsten et al. 2009; Zwijsen et al. 2011). Generally speaking, the freedom of users may be impeded due to the presence of sensors or transmission of data generated by H-IoT devices.

Privacy can be considered a prerequisite for autonomy (cf. Floridi 2016; Wachter 2017). Undesired sharing of information or intrusions into physical spaces or social relationships can impede a user's capacity to make decisions (Bowes et al. 2012; Essén 2008). H-IoT data can contribute to profiling of users as 'health impaired' or 'at-risk' (Rigby 2007; Percival and Hanson 2006; McLean 2011). In turn, this profiling influences the choices made available by other third parties with access to the profile (Kosta et al. 2010).

H-IoT used for chronic illness management can alternatively gradually reduce rather than outright impede user autonomy, for instance by automatically issuing alerts of abnormal behaviours, readings or emergencies. While undoubtedly important functions to ensure patient safety, alerts can similarly impact on a user's sense of self-reliance (Percival and Hanson 2006; Remmers 2010) when it is perceived that a carer or medical professional will be alerted whenever something goes wrong (Bowes et al. 2012; Fugger et al. 2007; Demiris 2009). Carers given access to the data collected by a H-IoT device can assess the patient's behaviour, such as whether a treatment plan is being correctly followed (De Bleser et al. 2011), or the user is engaging in risky behaviour. This type of oversight by carers can disrespect the patient's self-determination and autonomy (Remmers 2010). Dependent users may also experience changes to their relationships with carers (Palm et al. 2012). In this context, Kenner (2008) suggests, for example, that carers should assess when interventions based on H-IoT data could potentially infringe upon the user's rights to privacy and autonomy.

Consent and the uncertain value of H-IoT data

While recognising the inherent uncertainty of the future value of data in academic research and commercial analytics, manufacturers must nevertheless consider the potential value of data generated by their devices. Two related concerns must be addressed. First, does the device collect the minimal amount and types of data necessary to deliver the promised service, so as to minimize privacy risks to the user? Second, to what extent are users informed of the potential value and third party uses of the data they generate? The first concern has already been addressed above (see "Informational privacy" section).

Regarding the second, traditional models of informed consent are not directly applicable to H-IoT data. Terms of Service and other end-user agreements governing these applications tend to permit collection, aggregation, and analysis of usage and behavioural data without clear indications of how data will be used in the future, beyond general statements about third party access. H-IoT devices can generate 'invisible data' for which the user is unaware of the scope or granularity of parameters being measured (Peppet 2014; Denecke et al. 2015; Bietz et al. 2016). A lack of an explicit *informed* consent mechanism in end-user agreements between H-IoT manufacturers and users gives cause for concern (Fairfield and Shtein 2014), even when 'participants' are 'de-identified' (Ioannidis 2013), when the data generated are intended to be re-purposed for medical research or comparable consumer analytics (Taddeo 2016). Device manufacturers must design user agreements to represent fairly the uncertain value of data generated by users, and the potential for aggregation and linkage by third parties for both research and commercial purposes. Even if user agreements are designed in this way, the communication of limited but relevant and informative information based on user's context- and cohort-specific needs remains a challenge (Pasluosta et al. 2015).

Consent is normally granted for participation in a single study, not covering unrelated investigations resulting from sharing, aggregating, or even repurposing data within the wider research community (Choudhury et al. 2014, p. 4). Such 'single-instance consent' is challenged by new opportunities for secondary analysis based on linked and aggregated data, and which often reveal unforeseen connections and inferences (cf. Peppet 2014; Mittelstadt et al. 2016). This is a pressing problem. While the initial risks and benefits of adopting H-IoT can reasonably be presented to potential users, the future utility and invasiveness of the data (i.e. what the data can reveal about the private life of the user) cannot be known at the point of adoption (Clayton 2005; Choudhury et al. 2014; Kaye et al. 2015; Peppet 2014).[5] Invasive inferences can be made about users based on collected data, potentially resulting in discrimination or

[5] For further discussion of alternative models of informed consent, see: Mittelstadt and Floridi (2016).

exclusion from data-driven services, or decision-making based upon private knowledge the user would otherwise not choose to share (Peppet 2014; Haddadi et al. 2015; Kostkova et al. 2016). For example, secondary effects of pharmaceuticals can be identified by comparing data from multiple clinical trials as well as 'informal sources', such as incidental self-reporting via social media and search engine queries (Salathé et al. 2012). In this type of research, the connections that can be revealed by linking diverse datasets cannot be accurately predicted.

This uncertainty introduced by Big Data analytics means that single-instance consent is largely inadequate to foster the scientific value of data science in general, and H-IoT in particular. The uncertain risks of H-IoT should, however, be considered next to the potential benefits of aggregation and re-use, both for the user's direct healthcare and well-being and for the development of medical knowledge (Bietz et al. 2016).

Ownership and data access

Data subjects and controllers share vague 'ownership' rights regarding the redistribution and modification of H-IoT data (Kostkova et al. 2016). These rights are guaranteed through privacy and data protection law, and may require extension according to prevailing ethical ideals concerning privacy, autonomy, and the right to identity (cf. Floridi 2011). In Europe for example, data subjects retain rights guaranteed through privacy and data protection law to be 'kept in the loop' regarding data processing and storage (Tene and Polonetsky 2013), meaning that data subjects retain rights to be notified when data about them are created, modified or analysed, and must be provided means to access and correct errors or misinterpretations in the data and knowledge derived from it (Coll 2014). When legal requirements do not result in meaningful and practically useful access for data subjects (e.g. Wachter et al. 2017a), ethical principles can be drawn upon both to ground changes to the law and to argue that responsible data controllers will go above and beyond legal requirements to ensure meaningful access.

H-IoT protocols can be designed to meet ethical standards that extend beyond legal requirements, for example by allowing data subjects greater access or opportunities to modify or correct their data than required by data protection law. Superficially, such ethical standards can be connected to the legally recognised 'right to be forgotten',[6] insofar as similar rights to modify privately held personal data (as opposed to public links) could conceivably be granted as an oversight mechanism. Hypothetically, it has been argued that a right to 'self-determination' can ground such connected data rights (Coll 2014) to contrast the 'transparency asymmetry' that exists when consumers lack information about how data about them are "collected, analysed and used" (Coll 2014, p. 1259; Richards and King 2013). Background social prejudices, inequalities, and biases can have greater influence in data processing where subjects lack oversight (McNeely and Hahm 2014; Oboler et al. 2012).

Accessibility does not come without risks. For instance, it has been noted that unrestricted access to raw data may be harmful if subjects lack the necessary expertise or resources for interpretation (boyd and Crawford 2012; Coll 2014; Pasluosta et al. 2015). Misinterpretation is a concern when data are assessed without assistance, e.g. from a trained clinician, carer or data scientist (Watson et al. 2010). Furthermore, revision rights undermine the accuracy and integrity of datasets due to modifications made by data subjects.

Data subject rights to access and modify data are reliant upon the subject being aware of what data exist about her, who holds them, what they (potentially) mean, and how they are being used. Assuming such rights are sought, significant technical and practical barriers to their realisation exist. 'Big Data' requires significant computational power and storage, and advanced scientific know-how (Burrell 2016; Mittelstadt and Floridi 2016). As with any type of data science, technical expertise and background knowledge is required to make sense of the data being shared. Expecting data subjects to acquire the necessary skills to derive meaning from shared data is unreasonable (Andrejevic 2014). If meaningful access rights are sought, alternative arrangements and assistance must be available.

Data subjects, thus, face considerable barriers to accessing and understanding the meaning of data produced by H-IoT. Meaningful oversight and control of personal data are unrealistic expectations under these conditions (Mittelstadt and Floridi 2016). Gaps exist between the ideal protections for informational privacy and the actual capacity of data subjects to exercise meaningful control over their data (Andrejevic 2014). Without further assistance from data controllers, data subjects will remain unable to understand the meaning and scope of their data being processed or request modifications and corrections. Domain-specific requirements are needed that describe reasonable access rights and barriers to access. Consideration should also be given to the need to alter legal and ethical standards for data controllers to provide meaningful access. Data controllers can, for instance, explain how categories, profiles or other criteria are used to make sense of H-IoT data (cf. Hildebrandt and Gutwirth 2008), which tells data subjects

[6] For further details on the specification of the right to be forgotten by Google in the EU, see: Advisory Council to Google on the Right to be Forgotten (2015).

how they are being compared with other H-IoT users and patients. A full explanation of how a specific automated decision was reached based, at least in part, on H-IoT data is another option, albeit one currently lacking legal force (for a discussion of this problem in European data protection law, see Wachter et al. 2017a, b).

While modifications to data protection law are one possibility to the accessibility and visibility of H-IoT data collection and processing for data subjects, the development of ethical standards for data controllers handling H-IoT data may be more feasible in the short term. McNeely and Hahm (2014, p. 1654) have proposed a set of 'core principles of expanded data sharing' to be followed by "any system that is ultimately adopted for expanded access to participant-level data." The principles focus on several norms and concepts, including responsibility, privacy, equal treatment of all data requesters/trial sponsors, accountability of data controllers and requesters, the practicality of the system in terms of transparent and timely responses to data requests, and a lack of other such unnecessary barriers to access. Alternatively, Nunan and Di Domenico (2013) have recommended enforcing a 'right to be forgotten', a 'right to data expiry', and the 'ownership of a social graph' by data subjects. The first refers to the ability of data subjects to request that links to information about them be deleted. The second refers to the automatic deletion of unstructured data after a set period of time if they no longer have any commercial or research value.[7] The third will detail what data exist about an individual, when and how they were collected, and where they are stored.

It can also be argued that data subjects should be allowed to derive personal benefit from their data beyond the products or services provided by the data controller (Tene and Polonetsky 2013). If a right to benefit from data about oneself is recognised, subjects should arguably be offered "meaningful rights to access their data in a usable, machine-readable format" (Tene and Polonetsky 2013, p. 242). Such steps allow subjects to find individual benefits from the data they produce and communities (or aggregated datasets) in which their data reside (Lupton 2014b). Currently, data subjects tend not to benefit directly from analysis of data collected about them—users of Facebook, for instance, do not share in the revenue derived from targeted advertisements. The continuing development of products and services based on secondary analysis of personal data, such as that generated by H-IoT, will raise questions over ownership rights to intellectual property developed from H-IoT data. Similar to R&D for pharmaceuticals (Chapman et al. 2003; Petryna et al. 2006), data subjects can make a strong ethical (but not necessarily legal) claim to share in the benefits of products and services developed from their data.

Ethical issues for H-IoT mediated care

Other ethical problems with H-IoT focus on the impact on the delivery of healthcare and the maintenance or augmentation of norms of 'good practice' in medical and social care.

Social isolation

The use of H-IoT to manage health conditions at home or in residential care can contribute to social isolation of users. Visits from medical personnel and carers may be less necessary if daily monitoring of conditions is controlled by H-IoT (Demiris et al. 2004; Stowe and Harding 2010; Tiwari et al. 2010; Wu et al. 2012). Studies involving older people have revealed a concern that H-IoT will replace personal and social interactions with carers (Chan et al. 2008; McLean 2011; Palm 2011; Zwijsen et al. 2011; Wu et al. 2012) rather than merely supplementing them, as it is often promised. Collection of contextual information about a patient's condition via face-to-face interactions can be difficult to replicate with sensors (Percival and Hanson 2006; see "'Good' care and user well-being" section).

While a concern over increased social isolation was common, assistive homecare robots (which can in be considered H-IoT when Internet-enabled) and social networking features in clinical H-IoT have been proposed as solutions (Wu et al. 2012; Percival and Hanson 2006). Such solutions can only be considered sufficient if it is assumed that robots or social networking sufficiently replaces interactions between users and human carers. These different modes of interaction will not necessarily replicate face-to-face interactions, or similarly contribute to users' mental health and well-being, and this brings about some fundamental ethical problems concerning the nature and the scope of medical and health-care practitioners.

Decontextualisation of health and well-being

H-IoT is often promoted as a way to improve the efficiency and quality of both clinical care and long-term management of health and well-being. These benefits rely upon

[7] Although attempts to define concepts such as 'commercial' or 'research' value face theoretical and practical challenges, they nevertheless represent an attempt to realise meaningful rights of data access and control. This discussion will be particular relevant for Europe in the immediate future due to implementation of the General Data Protection Regulation from 2018, which grants notification duties for data controllers (Articles 13–14) access rights for data subjects (Article 15). The precise rights of data subjects and concomitant duties of data controllers and IoT providers created by these Articles will be clarified from 2018 onwards.

a number of factors, including the parameters by which 'good' care and health management are measured. One risk presented by H-IoT is the simplification of health and patient care to parameters and processes that can be easily measured or automated.

H-IoT can limit assessment of a patient's condition to a narrow range of easily measurable or quantifiable considerations, which could bias assessment towards an overly optimistic prediction of the technology's effects (Mittelstadt et al. 2014; Coeckelbergh 2013). Conditions can increasingly be modelled and monitored through data, supplementing or replacing verbal accounts and physical care (cf. Morris 1996; Edgar 2005). A key challenge lies in reflexive examination of the epistemic limits of these data representations of the patient, which pre-emptively restrict the physician's understanding of the patient's case by filtering it through the interpretive frameworks designed into the monitoring systems that have constructed the data representation (cf. Lyon 2003; Hildebrandt 2008). Monitoring data can be communicated to the care team and patient in varying degrees of complexity and completeness. When systems simplify or summarise the data prior to it reaching the care team or patient, the data become value-laden (cf. Gadamer 1976). Monitoring physiological parameters reproduces a certain conception of 'health', whereby a patient's condition is increasingly evaluated and understood in terms of parameters that can be monitored and related metrics. Devices that allow for continuous monitoring of blood pressure can, for example, change how 'high blood pressure' is classified compared to prior interval contingent measurements (Laurance 2011). Measurements which would indicate high blood pressure when measured once-off (for instance, in a doctor's office) may instead come to be understood as natural fluctuations within a normal range. A related risk exists that monitoring data will increasingly be seen as an 'objective' measure of health and well-being, thereby reducing the importance of contextual factors of health or the view of the patient as a socially embodied person (Haggerty and Ericson 2000). H-IoT may create a 'veneer of certainty', in which 'objective' monitoring data are taken to represent a true representation of the patient's situation, losing sight of the data collection context (Bauer 2004; Lupton 2013b, p. 398).

Assuming patients have a right to control over their personal data and inviolate construction of personal identity (cf. Floridi 2011), the obfuscation of such filtering processes and their normalizing effect on evaluations of health can be considered ethically problematic. The patient is unlikely and unable to be made aware of the categorisations and interpretations of the data that frame his treatment (Monahan and Wall 2007; Lupton 2012; Mittelstadt and Floridi 2016), yet she will be treated by medical professionals and institutions on the basis of this identity that has been constructed beyond her control or awareness.

A related problem concerns the quality of care provided to the patient, wherein H-IoT can be seen as ethically problematic if it undermines clinically effective or benevolent care. Monitoring data can complicate assessments of the patient's condition, which would otherwise rely upon physical examination and tacit knowledge (Lupton 2013a; Coeckelbergh 2013). A patient's condition has traditionally been understood through clinical tests and interactions, and the patient's verbal account. H-IoT data introduces a new source of information. The amount and complexity of monitoring data makes it difficult to identify when important contextual information is missing from monitoring records (cf. Knobel 2010). Reliance upon H-IoT data as a primary source of information about a patient's health can result in ignorance of aspects of the patient's health that cannot easily be monitored by H-IoT, such as their social, mental, and emotional state (Coeckelbergh 2013). 'Decontextualisation' of the patient's condition can occur as a result, wherein the patient loses some control over how her condition is presented and understood by clinicians and carers (Lupton 2013a; Coeckelbergh 2013; Stutzki et al. 2013). The risk is particularly acute when face-to-face encounters conducive to empathetic and compassionate care (cf. Gelhaus 2012a, b) are replaced by remote monitoring. Psychological aspects of well-being describable only by the patient would subsequently be lost from the clinical encounter (cf. Morris 1996; Barry et al. 2001; Edgar 2005), unless specifically requested through remote consultations or follow-up with the patient. Institutions and physicians may be tempted to 'close down' discourses with patients by placing greater importance on 'objective' H-IoT monitoring data than the patient's subjective experience and voice (Coeckelbergh 2013; Mittelstadt et al. 2014).

'Good' care and user well-being

All of these possibilities suggest H-IoT can routinely produce a poorer view of social and contextual factors of a patient's health, in particular relating to mental health and well-being (Lupton 2013a). Bauer (2004, p. 84) suggests that technologies which inhibit communication of "psychological signals and emotions" impede the physician's knowledge of the patient's condition, "retarding the establishment of a trusting and healing physician-patient relationship." Care providers may be less able to demonstrate understanding, compassion, and other desirable traits found within 'good' medical interactions in addition to applying their knowledge of medicine to the patient's case (cf. Pellegrino and Thomasma 1993; MacIntyre 2007; Beauchamp and Childress 2009). As a mediator placed between the physician and patient (Mittelstadt et al. 2014), H-IoT

changes the dependencies between clinicians and patients by turning some degree of the patient's ongoing care over to a technological artefact. At a minimum, responsive steps need to be taken to develop a trusting relationship between patients, medical professionals, and H-IoT manufacturers, for example by using monitoring as a way to initiate rather than replace dialogue between patient and doctor. The development of norms to govern H-IoT mediated or online medical communication may also help preserve the integrity of the doctor-patient relationship (Denecke et al. 2015).

Care via monitoring implies a loss of opportunities to develop trust and relational understanding between patient and carer, which traditionally develop via face-to-face care (Coeckelbergh 2013; Laplante and Laplante 2016). H-IoT can create epistemic and social distance between patients and health professionals. Such distance can be considered ethically problematic insofar as it contributes to misunderstanding of the patient's health and well-being beyond physiological measurements (Lupton 2015). At a minimum, responsive steps need to be taken to develop a trusting relationship, for example by using monitoring as a way to initiate rather than replace dialogue with the patient. Monitoring does not need to develop into a barrier to good care relationships in itself (Coeckelbergh 2013); H-IoT does not undermine 'good' healthcare out of necessity. Rather, H-IoT is ethically problematic insofar as it is used poorly, without the limitations of its measurements being acknowledged and corrected for in the user's overall care (Coeckelbergh 2013).

As a result of such qualitative differences in the types of care enabled by H-IoT, more efficient usage of limited healthcare resources can come at the cost of excellence-in-practice, or "craftsmanship" (Coeckelbergh 2013). A potential exists in professional healthcare for H-IoT to alter care relationships and displace responsibilities traditionally fulfilled by professional carers and clinicians. Despite this, existing academic discourse tends to conceive of the ethical possibilities of H-IoT in terms of harms and benefits for individual patients, clinicians, developers or medical organisations (Mittelstadt et al. 2013, 2014). As discussed above, some literature addresses the isolating effects of H-IoT, but further exploration of the normalizing effects and 'decontextualisation' of H-IoT data on medical encounters is badly needed.

Risks of non-professional care

Where H-IoT is used to reduce the burden on professional resources for social and medical care, a burden is implicitly shifted to family members, friends, and the community ('informal carers') to replace interpersonal and social interactions that would otherwise be lost. Additionally, informal carers can become, not necessarily willingly, the first point of contact for H-IoT alerts. Even if care duties are fully and readily accepted by informal carers, the same moral obligations that bind medical and social care professionals will not necessarily be met by informal carers (cf. Palm 2011), in part because informal care lacks a deontological code, moral and legal obligations, and training of medical professions. The nature of care experienced by the user is thus changed by H-IoT. Medical professionals have moral obligations placed upon them, for instance to act in the best interests of patients rather than self-interest or to not exploit the patient's vulnerability in seeking out medical care (cf. Pellegrino and Thomasma 1993). Professionals develop norms of good practice over time, and come to appreciate the needs of patients beyond the physiological. This practical wisdom and professionalism are lost when care is shifted to informal carers (Coeckelbergh 2013). Professionalism and craftsmanship may be eroded through an isolation of care workers from the patient and other health professionals, where face-to-face interactions are replaced or modified by technologically-mediated work, reducing opportunities for skill development, community, and character building within medicine (Coeckelbergh 2013).[8]

This change does not mean that non-professionals are 'bad' carers by default, or that patients will necessarily face greater risks from H-IoT mediated care. Informal carers can similarly develop norms of good practice over time. However, training in medical and social care emphasises the vulnerability of patients and the moral obligations placed upon professionals in these fields (Coeckelbergh 2013). This awareness will not automatically transfer to informal carers. When deploying H-IoT, it is critical to acknowledge the change and to re-evaluate what 'good' medical and social care look like when mediated by H-IoT, for instance by monitoring for deficiencies that impact both the patient's health and psychological well-being. The impact of H-IoT devices and services autonomously interacting with one another or communicating data to third parties will be particularly difficult to predict (Ebersold and Glass 2016).

Entering into a care relationship requires trust (Pellegrino and Thomasma 1993; Pellegrino 2002); whether trusting 'physician proxies' (e.g. monitoring service

[8] At first glance this appears to be an overreaction—after all, wearable 'wellness' monitors are not obviously meant to become part of an individual's healthcare. However, 'wellness' and 'medicine' share a common goal: to contribute to the healthy functioning of the individual. Wellness monitors work towards this end by facilitating preventative self-care, reflecting broader shifts in public health programmes towards personal responsibility for health. As suggested by the 'Quantified Self' movement, monitoring data contains within it the possibility of better health to be unlocked by analysis and behavioural change (Lupton 2013b). Patient empowerment and self-care movements (e.g. Ball and Lillis 2001; Lupton 2013a) thus increasingly link wellness with medicine and health.

providers) is wise can be determined only on a case-by-case basis. The moral obligations of the healing relationship (Pellegrino and Thomasma 1993) are displaced through the introduction of new devices or stakeholders that provide care, without clearly changing the patient's experience of illness (e.g. fear, helplessness, dependency) or their expectations of care and carers (Edgar 2005). The patient's 'vulnerable' position in the relationship (Pellegrino and Thomasma 1993) may not be evident to these new stakeholders or sustained throughout the relationship.

Users of H-IoT face new risks, many of which stem from inappropriate uses of collected data. Users may face unwanted personalised marketing and personalised insurance premiums (Percival and Hanson 2006; Kosta et al. 2010), exclusion from services or offerings due to limiting access to personal data (Brey 2005), or discrimination resulting from inferential analytics (Peppet 2014). To limit possibilities of data misuse and come closer to an ideal of informed consent, information about data retention and processing aims needs to be available to users before data are collected (Kosta et al. 2010).

Strong protection of users' informational privacy (see "Informational privacy" section) can help restore a balance by limiting such unwanted disturbances and exploitation, such as advertising based upon the user's medical history. Profiling, behavioural regulation, and social sorting all depend upon personal data (Kosta et al. 2010). Controlling data and information flows can thus enhance a user's autonomy and privacy by acting as a check on the power of medical organisations, data controllers, and researchers (Friedewald et al. 2007; Moncrieff et al. 2009).

These concerns suggest that the degree to which H-IoT will inhibit 'good' medical practice hinges upon the model of service. If delivery is handled entirely by existing care teams bound by the moral obligations of the healing relationship, the problems created by 'non-virtuous' stakeholders entering the relationship are reduced, albeit not eliminated. As it stands, patients' trust will be misplaced so long as equivalent norms of practice for providing healthcare-via-monitoring remain unspecified. Such norms require the communication of role-based obligations to new care providers, both informal carers and providers of H-IoT devices and services, including dialogue to define appropriate codes of conduct and related principles of good practice in H-IoT mediated informal care (Palm 2011; Mittelstadt et al. 2014). Alternatively, it can be argued that 'good medicine' (cf. MacIntyre 2007; Pellegrino and Thomasma 1993) should increasingly be re-defined around patients exercising greater control over their care in H-IoT-mediated relationships in the future to counteract reduced involvement of clinicians (as moral practitioners in medicine). The ideal of 'self-responsibility' can mean that patients gain greater autonomy in the healing relationship at the cost of increased responsibility for their health and well-being.

Conclusion

This paper reviews ethical problems arising from the design and deployment of H-IoT as described in the relevant literature. These problems can broadly be distinguished by their focal point on devices, data protocols, or medical and social care. The range of ethical issues described in this article are intended as a starting point for further discussion and specification of moral responsibilities and principles for responsible design and deployment of H-IoT. The discussion should be carried on in collaboration with designers of H-IoT devices and protocols targeting specific diseases, patient populations, and functionality.

Many ethical issues face both the design and deployment of H-IoT in healthcare. While some issues can be addressed by choices in the design process, many manifest in the actions and responsibilities of H-IoT providers post-deployment. H-IoT can be used to mediate healthcare and traditional medical relationships among patients, doctors, medical institutions, and professionals. Informal carers and private providers of H-IoT devices and services can increasingly be involved in the delivery of care and management of health. Medical researchers also have a stake in making sense of and creating value from the data produced by H-IoT (Denecke et al. 2015). Making explicit the expectations placed on each of these stakeholders in H-IoT mediated healthcare, broadly interpreted, can go some way to mitigating many of the post-deployment concerns described here.

What remains unclear is precisely how the moral responsibilities of medical care transfer to and are acknowledged by non-medical professionals. To address this issue going forward, it is necessary to describe how the moral responsibilities of medical care can be responsibly and fairly transferred to non-medical professionals contributing to the provision of care mediated by H-IoT.

In discussing the future ethical impact of H-IoT, one should not ignore potential benefits. Access to care can be increased for groups traditionally marginalised due to geographical distance, communicative abilities, or social status (e.g. Bauer 2004). Patient safety and engagement with medical care and health outcomes can also benefit from access to detailed personal health data records and feedback. Medical research can also benefit from the wealth of longitudinal, granular data produced by H-IoT, although data protocols that permit responsible but permissive sharing of data are key.

Despite these potential benefits, better understanding of patient attitudes towards self-care and self-responsibility

enacted through technologies such as H-IoT is required to assess the technology's impact on the delivery of healthcare, and to define adequate norms for good medical and social care. The existing assumption is that patients will welcome H-IoT if it is presented as improving their autonomy, the management of health and well-being, and the quality of healthcare. Whether patients will accept the underlying sense of self-responsibility and changes to professional and informal care remains unclear. The ethical themes discussed here provide a lens to highlight such issues in future discourses over ethically acceptable design and deployment for H-IoT.

Acknowledgements Preparation of this article benefitted greatly from the insightful comments and review provided by Dr. Mariarosaria Taddeo and Prof. Luciano Floridi, and from the anonymous reviewers at Ethics and Information Technology. The author is deeply indebted for their input which has significantly improved the article's quality.

Funding This article is a deliverable of the Data Analysis in IoT Solutions for Healthcare (DASH) project, part of the PETRAS internet of things research hub. PETRAS is funded by the Engineering and Physical Sciences Research Council (EPSRC), Grant Agreement No. EP/N023013/1.

References

Advisory Council to Google on the Right to be Forgotten. (2015). *Report of the Advisory Council to Google on the Right to Be Forgotten. Google Docs*. https://drive.google.com/file/d/0B1UgZshetMd4cEI3SjlvV0hNbDA/view?pli=1&usp=embed_facebook.

Agrafioti, F., Bui, F. M., & Hatzinakos, D. (2011). Medical biometrics in mobile health monitoring. *Security and Communication Networks, 4*, 525–539. doi:10.1002/sec.227.

Ahamed, S. I., Talukder, N., & Haque, M. M. (2007a). Privacy challenges in context-sensitive access control for pervasive computing environment. *In 4th Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, MobiQuitous 2007*. Philadelphia, PA. http://www.scopus.com/inward/record.url?eid=2-s2.0-50249180369&partnerID=40&md5=da4e8dd7956060a59a64ebf6dac97ecf.

Ahamed, S. I., Talukder, N., & Kameas, A. D. (2007b). Towards privacy protection in pervasive healthcare. In 296–303. *3rd IET International Conference on Intelligent Environments, IE'07*. Ulm. http://www.scopus.com/inward/record.url?eid=2-s2.0-67649784659&partnerID=40&md5=1317173c09f4221e24e19e389dd6f599.

Andrejevic, Mark (2014). Big data, big questions| the big data divide. *International Journal of Communication, 8*(0), 17.

Armac, I., Panchenko, A., Pettau, M., & Retkowitz, D. 2009. Privacy-friendly smart environments. In, 425–431. *NGMAST 2009–3rd International Conference on Next Generation Mobile Applications, Services and Technologies*. Cardiff. http://www.scopus.com/inward/record.url?eid=2-s2.0-74049140815&partnerID=40&md5=d531f04758ab995a44db1251d1149771.

Bagüés, S. A., Zeidler, A., Klein, C., Valdivielso, F., & Matias, R. (2010). Enabling personal privacy for pervasive computing environments. *Journal of Universal Computer Science, 16*, 341–371.

Bagüés, S. A., Zeidler, A., Valdivielso, F., & Matias, R. (2007a). Disappearing for a while: Using white lies in pervasive computing. In *Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society, 80–83. 6th ACM Workshop on Privacy in the Electronic Society, WPES'07, Held in Association with the 14th ACM Computer and Communications Security Conference*. Alexandria, VA. http://www.scopus.com/inward/record.url?eid=2-s2.0-74049138834&partnerID=40&md5=85eabfb98cfe5d40f843c493ea3d460a.

Bagüés, S. A., Zeidler, A., Valdivielso, F., & Matias, R. (2007b). Sentry@Home-Leveraging the smart home for privacy in pervasive computing. *International Journal of Smart Home, 1*, 129–146.

Baldini, G., Botterman, M., Neisse, R., & Tallacchini, M. (2016). Ethical design in the internet of things. *Science and Engineering Ethics*. doi:10.1007/s11948-016-9754-5.

Ball, M. J., & Lillis, J. (2001). E-Health: transforming the physician/patient relationship. *International Journal of Medical Informatics, 61*, 1–10. doi:10.1016/s1386-5056(00)00130-1.

Bandyopadhyay, Debasis, Jaydip Sen (2011). Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications, 58*(1), 49–69. doi:10.1007/s11277-011-0288-5.

Barry, C. A., Stevenson, F. A., Britten, N., Barber, N., & Bradley, C. P. (2001). Giving voice to the lifeworld. more humane, more effective medical care? A qualitative study of doctor-patient communication in general practice. *Social Science and Medicine, 53*, 487–505. doi:10.1016/s0277-9536(00)00351-8.

Bauer, K. (2004). 'Cybermedicine and the moral integrity of the physician–patient relationship'. *Ethics and Information Technology, 6*(2), 83–91.

Beauchamp, T. L., Childress, J. F. (2009). *Principles of biomedical ethics*. New York: Oxford University Press.

Beaudin, J., Intille, S., & Morris, M. 2006. To track or not to track: user reactions to concepts in longitudinal health monitoring. *Journal of Medical Internet Research*. doi:10.2196/jmir.8.4.e29.

Bietz, M. J., Bloss, C. S., Calvert, S., Godino, J. G., Gregory, J., Claffey, M. P., et al. (2016). Opportunities and challenges in the use of personal health data for health research. *Journal of the American Medical Informatics Association, 23*(e1): e42–e48. doi:10.1093/jamia/ocv118.

Bohn, J, Coroamă, V., Langheinrich, M., Mattern, F., & Rohs, M. (2005). Social, economic, and ethical implications of ambient intelligence and ubiquitous computing. Http://Www.vs.Inf.Ethz.Ch/Publ/Papers/Socialambient.Pdf, 2004. Institute for Pervasive Computing'. CiteSeerX. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.70.2159.

Bowes, A., Dawson, A., & Bell A. (2012). Ethical implications of lifestyle monitoring data in ageing research. *Information, Communication & Society, 15*(1), 5–22. doi:10.1080/1369118X.2010.530673.

Boyd, D., & Crawford, K. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information Communication & Society, 15*(5), 662–679. doi:10.1080/1369118X.2012.678878.

Brey, P. (2005). Freedom and privacy in ambient intelligence. *Ethics and Information Technology, 7*(3), 157–166.

Burrell, J. (2016). How the machine "thinks": Understanding opacity in machine learning algorithms. *Big Data & Society*. doi:10.1177/2053951715622512.

Busnel, P., & Giroux, S. (2010). Security, privacy, and dependability in smart homes: A pattern catalog approach. In *Vol. 6159 LNCS. 8th International Conference on Smart Homes and Health Telematics, ICOST 2010*. Seoul. http://www.scopus.com/inward/record.url?eid=2-s2.0-77955446331&partnerID=40&md5=b20fa2bca706ec75ab071f1fcd3554c8.

Caine, K. E., Fisk, A. D., & Rogers, W. A. 2006. Benefits and privacy concerns of a home equipped with a visual sensing system: A perspective from older adults. In 180–184. *50th Annual Meeting of the Human Factors and Ergonomics Society, HFES 2006*. San Francisco. http://www.scopus.com/inward/record.url?eid=2-s2.0-44349169380&partnerID=40&md5=2b10e6a27ff9837d6d5b4c5c6793efbe.

Center for Devices and Radiological Health. (2014). Content of premarket submissions for management of cybersecurity in medical devices. Washington, D.C.: U.S. Department of Health and Human Services. http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

Chakraborty, S., Choi, H., & Srivastava, M. B. (2011). Demystifying privacy in sensory data: A QoI based approach. In 38–43. *2011 9th IEEE International Conference on Pervasive Computing and Communications Workshops, PERCOM Workshops 2011*. Seattle. http://www.scopus.com/inward/record.url?eid=2-s2.0-79958057222&partnerID=40&md5=e907b7a413b53870811659ac9d8b0682.

Chan, M., Campo, E., Estève, D., & Fourniols, J. Y. (2009). Smart homes—current features and future perspectives. *Maturitas, 64*(2), 90–97. doi:10.1016/j.maturitas.2009.07.014.

Chan, M., Estève, D., Escriba, C., & Campo, E. (2008). A review of smart homes: Present state and future challenges. *Computer Methods and Programs in Biomedicine, 91*, 55–81. doi:10.1016/j.cmpb.2008.02.001.

Chapman, S., Reeve, E., Rajaratnam, G. & Neary, R. (2003). Setting up an outcomes guarantee for pharmaceuticals: new approach to risk sharing in primary care. *British Medical Journal, 326*(7391), 707.

Choudhury, S., Fishman, J. R., McGowan, M. L., & Juengst, E. T. (2014). Big data, open science and the brain: Lessons learned from genomics. *Frontiers in Human Neuroscience, 8*, 239. doi:10.3389/fnhum.2014.00239.

Clarke, Andrew, Robert Steele (2015). Smartphone-based public health information systems: Anonymity, privacy and intervention. *Journal of the Association for Information Science & Technology, 66*(12), 2596–2608. doi:10.1002/asi.23356.

Clayton, E. W. (2005). Informed consent and Biobanks. *Journal of Law, Medicine & Ethics, 33*(1), 15–21. doi:10.1111/j.1748-720X.2005.tb00206.x.

Coeckelbergh, M. (2013). E-care as craftsmanship: Virtuous work, skilled engagement, and information technology in health care. *Medicine, Health Care and Philosophy, 16*(4), 807–816. doi:10.1007/s11019-013-9463-7.

Coll, S. (2014). Power, knowledge, and the subjects of privacy: understanding privacy as the ally of surveillance. *Information Communication & Society, 17*(10), 1250–1263. doi:10.1080/1369118X.2014.918636.

Costa, F. F. (2014). Big data in biomedicine. *Drug Discovery Today, 19*(4), 433–440. doi:10.1016/j.drudis.2013.10.012.

Coughlin, J. F., D'Ambrosio, L. A., Reimer, B., & Pratt, M. R. 2007. Older adult perceptions of smart home technologies: Implications for research, policy & market innovations in healthcare. In *Proceedings of the 29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2007. EMBS 2007*, 1810–1815. doi:10.1109/IEMBS.2007.4352665.

Coughlin, J. F., Lau, J., D'Ambrosio, L. A., & Reimer, B. (2009). Adult children's perceptions of intelligent home systems in the care of elderly parents. In *3rd International Convention on Rehabilitation Engineering and Assistive Technology, ICREATE'09*. http://www.scopus.com/inward/record.url?eid=2-s2.0-70449639811&partnerID=40&md5=97a0f07bfa75dc9a0eaa8e29217ed9e0.

Courtney, K. L. (2008). Privacy and senior willingness to adopt smart home information technology in residential care facilities. *Methods of Information in Medicine, 47*, 76–81. doi:10.3414/me9104.

Courtney, K. L., Demiris, G., & Hensel, B. K. (2007). Obtrusiveness of information-based assistive technologies as perceived by older adults in residential care facilities: A secondary analysis. *Medical Informatics and the Internet in Medicine, 32*, 241–249. doi:10.1080/14639230701447735.

Courtney, K. L., Demiris, G., Rantz, M., & Skubic, M. (2008). Needing smart home technologies: The perspectives of older adults in continuing care retirement communities. *Informatics in Primary Care, 16*, 195–201.

Currie, J. 2013. "Big data" versus "big brother": On the appropriate use of large-scale data collections in pediatrics'. *Pediatrics* 131: S127–S132. doi:10.1542/peds.2013-0252c.

De Bleser, L., De Geest, S., Vincke, B., Ruppar, T., Vanhaecke, J., & Dobbels, F. (2011). How to test electronic adherence monitoring devices for use in daily life: A conceptual framework. *CIN, 29*(9), 489–495.

Demiris, G., Rantz, M., Aud, M., Marek, K., Tyrer, H., Skubic, M., et al. (2004). Older adults' attitudes towards and perceptions of 'smart home' technologies: A pilot study. *Informatics for Health and Social Care, 29*, 87–94. (**citeulike-article-id:6074761**).

Demiris, G. (2009). Privacy and social implications of distinct sensing approaches to implementing smart homes for older adults. In *Conference Proceedings: Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE Engineering in Medicine and Biology Society. Conference* (pp. 4311–4314). http://www.scopus.com/inward/record.url?eid=2-s2.0-77951231210&partnerID=40&md5=4c55b833f18f571a9142982593f93f24.

Demiris, G., & Hensel, B. K. (2009). "Smart homes" for patients at the end of life. *Journal of Housing for the Elderly, 23*, 106–115. doi:10.1080/02763890802665049.

Denecke, K., Bamidis, P., Bond, C., Gabarron, E., Househ, M., Lau, A. Y. S. et al. (2015). Ethical issues of social media usage in healthcare. *IMIA Yearbook of Medical Informatics 10*(1), 137–47.

Dhukaram, A. V., Baber, C., Elloumi, L., Van Beijnum, B. J., & De Stefanis, P. (2011). End-user perception towards pervasive cardiac healthcare services: benefits, acceptance, adoption, risks, security, privacy and trust. In 478–484. *5th International Conference on Pervasive Computing Technologies for Healthcare and Workshops, Pervasive Health 2011*. Dublin. http://www.scopus.com/inward/record.url?eid=2-s2.0-80054938130&partnerID=40&md5=72d5cd50d9607fcde8a2fe9e0fb6209d.

Dorsten, A. M., Sifford, S. K., Bharucha, A., Mecca, L. P., & Wactlar, H. (2009). Ethical perspectives on emerging assistive technologies: insights from focus groups with stakeholders in long-term care facilities. *Journal of Empirical Research on Human Research Ethics, 4*, 25–36. doi:10.1525/jer.2009.4.1.25.

Ebersold, K., Glass, R. (2016). The internet of things: A cause for ethical concern. *Issues in Information Systems*. http://www.iacis.org/iis/2016/4_iis_2016_145-151.pdf.

Edgar, A. (2005). The expert patient: Illness as practice. *Medicine, Health Care and Philosophy, 8*(2), 165–171.

E-Health Insider. (2014). The year of the wearable. http://www.ehi.co.uk/insight/analysis/1404/the-year-of-the-wearable.

Elkhodr, M., Shahrestani, S., & Cheung, H. (2011). Ubiquitous health monitoring systems: addressing security concerns. *Journal of Computer Science, 7*, 1465–1473. doi:10.3844/jcssp.2011.1465.1473.

Empirica, W. R. C. (2010). *ICT & Ageing-European Study on Users, Markets and Technologies: Final Report'* European Commission. http://www.ict-ageing.eu/ict-ageing-website/wp-content/uploads/2010/D18_final_report.pdf.

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 & Medicine, 67*, 128–136. doi:10.1016/j.socscimed.2008.03.005.

Fairfield, J., Shtein, H. (2014). Big data, big problems: Emerging issues in the ethics of data science and journalism. *Journal of Mass Media Ethics, 29*(1), 38–51. doi:10.1080/08900523.2014.863126.

Floridi, L. (2011). The informational nature of personal identity. *Minds and Machines, 21*(4), 549–566. doi:10.1007/s11023-011-9259-6.

Floridi, L. (2016). On human dignity as a foundation for the right to privacy. *Philosophy and Technology, 29*(4), 307–312.

Friedewald, M., Vildjiounaite, E., Punie, Y., & Wright, D. (2007). Privacy, identity and security in ambient intelligence: A scenario analysis. *Telematics and Informatics, 24*(1), 15–29. doi:10.1016/j.tele.2005.12.005.

Fugger, E., Prazak, B., Hanke, S., & Wassertheurer, S. 2007. Requirements and ethical issues for sensor-augmented environments in Elderly care. Vol. 4554 LNCS. *4th International Conference on Universal Access in Human-Computer Interaction, UAHCI 2007*. Beijing.

Gadamer, H. G. (1976). *The historicity of understanding*. Harmondsworth: Penguin Books Ltd.

Gadamer, H. G. (2004). *Truth and method*. New York: Continuum International Publishing Group.

Garcia-Morchon, O., Falck, T., Heer, T., & Wehrle, K. (2009). Security for pervasive healthcare. In *2009 6th Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, MobiQuitous 2009*. Toronto. http://www.scopus.com/inward/record.url?eid=2-s2.0-72749094993&partnerID=40&md5=211a0a60d270e569349b0177265e29cd.

Garcia-Morchon, O., Falck, T., & Wehrle, K. (2011). Sensor network security for pervasive e-health. *Security and Communication Networks, 4*, 1257–1273. doi:10.1002/sec.247.

Gaul, S., Ziefle, M. (2009). Smart home technologies: Insights into generation-specific acceptance motives. In *HCI and Usability for E-Inclusion, edited by Andreas Holzinger and Klaus Miesenberger, 312–332. Lecture Notes in Computer Science 5889*. Berlin: Springer. http://link.springer.com/chapter/10.1007/978-3-642-10308-7_22.

Gelhaus, P. (2012a). The desired moral attitude of the physician: (I) Empathy. *Medicine, Health Care and Philosophy, 15*(2), 103–113. doi:10.1007/s11019-011-9366-4.

Gelhaus, P. (2012b). The desired moral attitude of the physician: (II) Compassion. *Medicine, Health Care and Philosophy, 15*(4), 397–410. doi:10.1007/s11019-011-9368-2.

Giannotti, F., Saygin, Y. (2010). Privacy and security in ubiquitous knowledge discovery. *Lecture Notes in Computer Science*. Berlin: Springer. doi:10.1007/978-3-642-16392-0_5.

Greenfield, A. (2008). Some guidelines for the ethical development of ubiquitous computing. *Philosophical Transactions of the Royal Society A, 366*(1881), 3823–2831. doi:10.1098/rsta.2008.0123.

Haddadi, H., Ofli, F., Mejova, Y., Weber, I., & Srivastava, J. (2015). 360-Degree quantified self. In 587–592. *IEEE*. doi:10.1109/ICHI.2015.95.

Haggerty, K. D., Ericson, R. V. (2000). The surveillant assemblage. *The British Journal of Sociology, 51*(4), 605–622. doi:10.1080/00071310020015280.

Hansson, M. G. (2009). Ethics and biobanks. *British Journal of Cancer, 100*(1), 8–12. doi:10.1038/sj.bjc.6604795.

Henderson, C., Knapp, M., Fernandez, J.-L., Beecham, J., Hirani, S. P. Cartwright, M., et al. (2013). Cost effectiveness of telehealth for patients with long term conditions (whole systems demonstrator telehealth questionnaire study): Nested economic evaluation in a pragmatic, cluster randomised controlled trial. *BMJ, 346*, f1035–f1035. doi:10.1136/bmj.f1035.

Hensel, B. K., Demiris, G., & Courtney, K. L. (2006). Defining obtrusiveness in home telehealth technologies: A conceptual framework. *Journal of the American Medical Informatics Association, 13*, 428–431. doi:10.1197/jamia.M2026.

Henze, M., Hermerschmidt, L., Kerpen, D., Häußling, R., Rumpe, B., & Wehrle, K. (2016). A comprehensive approach to privacy in the cloud-based internet of things. *Future Generation Computer Systems, 56*, 701–718. doi:10.1016/j.future.2015.09.016.

Higuchi, N. (2013). Three challenges in advanced medicine. *Japan Medical Association Journal, 56*(6), 437–447.

Hildebrandt, M. (2008). Defining profiling: A new type of knowledge?. In M. Hildebrandt & S. Gutwirth (Eds.) *Profiling the European citizen* (pp. 17–45). Dordrecht: Springer. http://link.springer.com/chapter/10.1007/978-1-4020-6914-7_2.

Hildebrandt, M., & Gutwirth, S. (2008). *Profiling the European citizen*. Dordrecht: Springer.

Huckvale, K., Prieto, J. T., Tilney, M., Benghozi, P. J. & Car, J. (2015). Unaddressed privacy risks in accredited health and wellness apps: a cross-sectional systematic assessment. *BMC Medicine, 13*, 214. doi:10.1186/s12916-015-0444-y.

Ioannidis, J. P. A. (2013). Informed consent, big data, and the oxymoron of research that is not research'. *American Journal of Bioethics, 13*(4), 40–42. doi:10.1080/15265161.2013.768864.

Jea, D., Liu, J., Schmid, T., & Srivastava, M. (2008). Hassle free fitness monitoring. In *2nd International Workshop on Systems and Networking Support for Health Care and Assisted Living Environments, HealthNet'08*. Breckenridge. http://www.scopus.com/inward/record.url?eid=2-s2.0-70349112153&partnerID=40&md5=65ede36cbc6922ee8365f8685b9403cd.

Jiya, T. (2016). A realisation of ethical concerns with smartphone personal health monitoring apps. *ACM SIGCAS Computers and Society, 45*(3), 313–317.

Kaye, Jane, Whitley, E. A., Lund, D., Morrison, M., Teare, H. & Karen Melham (2015). Dynamic consent: A patient interface for twenty-first century research networks. *European Journal of Human Genetics, 23*(2), 141–146. doi:10.1038/ejhg.2014.71.

Kenner, A. M. (2008). 'Securing the elderly body: Dementia, surveillance, and the politics of "aging in place'. *Surveillance & Society, 5*, 252–269.

Knobel, C. P. (2010). *Ontic occlusion and exposure in sociotechnical systems*. Pittsburgh: University of Pittsburgh. http://deepblue.lib.umich.edu/handle/2027.42/78763.

Kosta, E., Pitkänen, O., Niemelä, M., & Kaasinen, E. (2010). Mobile-centric ambient intelligence in health- and homecare-anticipating ethical and legal challenges. *Science and Engineering Ethics, 16*, 303–323.

Kostkova, P., Brewer, H., de Lusignan, S., Fottrell, E., Goldacre, B., Hart, G., et al. (2016). Who owns the data? Open data for healthcare. *Frontiers in Public Health*. doi:10.3389/fpubh.2016.00007.

Landau, R., Werner, S., Auslander, G. K., Shoval, N., & Heinik, J. (2010). What do cognitively intact older people think about

the use of electronic tracking devices for people with dementia? A preliminary analysis. *International Psychogeriatrics, 22*, 1301–1309.

Laplante, P. A., Laplante, N. (2016). The internet of things in healthcare: Potential applications and challenges. *IT Professional, 18*(3), 2–4.

Laurance, J. (2011). Revolutionary "wrist watch" to monitor high blood pressure. *The Independent*. http://www.independent.co.uk/life-style/health-and-families/health-news/revolutionary-wrist-watch-to-monitor-high-blood-pressure-2220650.html.

Leone, A., Diraco, G., & Siciliano, P. (2011). Topological and volumetric posture recognition with active vision sensor in AAL Contexts. In 110–114. *4th IEEE International Workshop on Advances in Sensors and Interfaces, IWASI 2011*. Savelletri di Fasano, Brindisi. http://www.scopus.com/inward/record.url?eid=2-s2.0-80052912635&partnerID=40&md5=73df8346c8100079e408eb255f47c961.

Little, L., & Briggs, P. (2009). Pervasive healthcare: The elderly perspective. In *2nd International Conference on PErvasive Technologies Related to Assistive Environments, PETRA 2009*. Corfu. http://www.scopus.com/inward/record.url?eid=2-s2.0-70450235243&partnerID=40&md5=8e09eaa23fd61ef86a45f904c7451b03.

Lomas, C. (2009). Telehealth system slashes hospital admissions in COPD patients. http://www.nursingtimes.net/nursing-practice/clinical-zones/copd/telehealth-system-slashes-hospital-admissions-in-copd-patients/5005885.article.

Lupton, D. (2012). M-health and health promotion: The digital cyborg and surveillance society. *Social Theory & Health, 10*(3), 229–244.

Lupton, D. (2013a). The digitally engaged patient: Self-monitoring and self-care in the digital health era. *Social Theory & Health, 11*(3), 256–270.

Lupton, D. (2013b). Quantifying the body: Monitoring and measuring health in the age of mHealth technologies. *Critical Public Health, 23*(4), 393–403.

Lupton, D. (2014a). The commodification of patient opinion: The digital patient experience economy in the age of big data. *Sociology of Health & Illness, 36*(6), 856–869. doi:10.1111/1467-9566.12109.

Lupton, D. (2014b). The commodification of patient opinion: The digital patient experience economy in the age of big data. *Sociology of Health & Illness, 36*(6), 856–869. doi:10.1111/1467-9566.12109.

Lupton, D. (2015). Health promotion in the digital era: A critical commentary. *Health Promotion International, 30*(1), 174–183. doi:10.1093/heapro/dau091.

Lyon, D. (2003). *Surveillance as social sorting: Privacy, risk, and digital discrimination*. London: Routledge.

MacIntyre, Alasdair. 2007. *After virtue: A study in moral theory* (3rd ed.). London: Gerald Duckworth & Co Ltd.

Mana, M., Feham, M., & Bensaber, B. A. (2011). Trust key management scheme for wireless body area networks. *International Journal of Network Security, 12*, 75–83.

Marx, Gary T (2001). Murky conceptual waters: The public and the private. *Ethics and Information Technology, 3*(3), 157–169.

Massacci, F., Nguyen, V. H., & Saidane, A. (2009). No purpose, no data: goal-oriented access control forambient assisted living. In 53–57. *1st ACM Workshop on Security and Privacy in Medical and Home-Care Systems, SPIMACS'09, Co-Located with the 16th ACM Computer and Communications Security Conference, CCS'09*. Chicago. http://www.scopus.com/inward/record.url?eid=2-s2.0-74049137043&partnerID=40&md5=98e37b22f5acce7ffaf8f6bdac154020.

Master, Zubin, Lisa Campo-Engelstein, Timothy Caulfield (2014). Scientists' perspectives on consent in the context of biobanking research. *European Journal of Human Genetics*. doi:10.1038/ejhg.2014.143.

Mathaiyan, J., Chandrasekaran, A., Davis, S. (2013). Ethics of genomic research. *Perspectives in Clinical Research, 4*(1), 100. doi:10.4103/2229-3485.106405.

McGuire, A. L., Colgrove, J., Whitney, S. N., Diaz, C. M., Bustillos, D., & Versalovic, J. (2008). Ethical, legal, and social considerations in conducting the human microbiome project. *Genome Research, 18*(12), 1861–1864. doi:10.1101/gr.081653.108.

McLean, Athena (2011). Ethical frontiers of ict and older users: cultural, pragmatic and ethical issues. *Ethics and Information Technology, 13*, 313–326. doi:10.1007/s10676-011-9276-4.

McNeely, C. L., & Hahm, J. O. (2014). The big (data) bang: Policy, prospects, and challenges. *Review of Policy Research, 31*(4), 304–310. doi:10.1111/ropr.12082.

Melenhorst, Anne-Sophie, Arthur D Fisk, Elizabeth D Mynatt, & Wendy A Rogers (2004). Potential intrusiveness of aware home technology: perceptions of older adults. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 48*, 266–270. doi:10.1177/154193120404800209.

Mitseva, A., Wardana, S. A., & Prasad, N. R. (2008). Context-aware privacy protection for wireless sensor networks in hybrid hierarchical architecture. In 773–78. *International Wireless Communications and Mobile Computing Conference, IWCMC 2008*. Crete. http://www.scopus.com/inward/record.url?eid=2-s2.0-52949130679&partnerID=40&md5=13e5c8cf6189923271c4ac6b216388e2.

Mittelstadt, B., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*. doi:10.1177/2053951716679679.

Mittelstadt, B., Fairweather, N. B., McBride, N., Shaw, M. (2011). Ethical issues of personal health monitoring: A literature review. In *ETHICOMP 2011 Conference Proceedings, 313–321*. Sheffield, UK.

Mittelstadt, B., Fairweather, N. B., McBride, N., Shaw, M. (2013). Privacy, risk and personal health monitoring. In *ETHICOMP 2013 Conference Proceedings*, (340–351). Kolding, Denmark.

Mittelstadt, B., Fairweather, N. B., Shaw, M., McBride, N. (2014). The ethical implications of personal health monitoring. *International Journal of Technoethics, 5*(2), 37–60.

Mittelstadt, B., Floridi, L. (2016). The ethics of big data: Current and foreseeable issues in biomedical contexts. *Science and Engineering Ethics, 22*(2), 303–341. doi:10.1007/s11948-015-9652-2.

Monahan, T., Wall, T. (2007). Somatic surveillance: Corporeal Control through information networks. *SSOAR*. http://nbn-resolving.de/urn:nbn:de:0168-ssoar-64160.

Moncrieff, S., Venkatesh, S., & West, G. (2009). A framework for the design of privacy preserving pervasive healthcare. In 1696–1699. *IEEE International Conference on Multimedia and Expo, ICME 2009*. New York. http://www.scopus.com/inward/record.url?eid=2-s2.0-70449589964&partnerID=40&md5=5fb4b46981d67f1d9a8d9387fd336acb.

Morris, D. B (1996). About suffering: Voice, genre, and moral community. *Daedalus, 125*(1), 25–45.

Nefti, S., Manzoor, U., & Manzoor, S. (2010). Cognitive agent based intelligent warning system to monitor patients suffering from dementia using ambient assisted living. In 92–97. *2010 International Conference on Information Society, i-Society 2010*. London. http://www.scopus.com/inward/record.url?eid=2-s2.0-80053373735&partnerID=40&md5=bd698fa210589c797f3dac10374cba8f.

Neild, I., Heatley, D. J. T., Kalawsky, R. S., & Bowman, P. A. (2004). Sensor networks for continuous health monitoring.

BT Technology Journal, 22(3), 130–139. doi:10.1023/B:BTTJ.0000047127.01462.49.

Nunan, D., Di Domenico, M. (2013). Market research and the ethics of big data. *International Journal of Market Research, 55*(4), 505. doi:10.2501/IJMR-2013-015.

Oboler, Andre, Welsh, K., & Cruz, L. (2012). The danger of big data: Social media as computational social science. *First Monday*. https://www.scopus.com/inward/record.url?eid=2-s2.0-84867308941&partnerID=40&md5=0e4cb2f657154c7f82a76c2a657259ab.

Ojasalo, J., Seppälä, H., Suomalainen, N. & Moonen, R. (2010). Better technologies and services for smart homes of disabled people: Empirical findings from an explorative study among intellectually disabled. In 1:V1251–1259. *2nd International Conference on Software Technology and Engineering, ICSTE 2010*. San Juan, PR. http://www.scopus.com/inward/record.url?eid=2-s2.0-78650035878&partnerID=40&md5=626a633c724af05d2d9953c4e5908d0a.

Pallapa, G., Roy, N., & Das, S. (2007). Precision: Privacy enhanced context-aware information fusion in ubiquitous healthcare. In *ICSE 2007 Workshops: First International Workshop on Software Engineering for Pervasive Computing Applications, Systems, and Environments, SEPCASE'07*. Minneapolis, MN. http://www.scopus.com/inward/record.url?eid=2-s2.0-38549097246&partnerID=40&md5=8fad28c8c1b83c25305adc6779428e19.

Palm, E. (2011). Who cares? Moral obligations in formal and informal care provision in the light of ICT-based home care. *Health Care Analysis*. doi:10.1007/s10728-011-0199-3.

Palm, E., Nordgren, A., Verweij, M., & Collste, G. (2012). Ethically sound technology? Guidelines for interactive ethical assessment of personal health monitoring. *Studies in Health Technology and Informatics, 187*, 105–114.

Pasluosta, C. F., Gassner, H., Winkler, J., Klucken, J., & Eskofier, B. M. (2015). An emerging era in the management of Parkinson's disease: Wearable technologies and the internet of things. *IEEE Journal of Biomedical and Health Informatics, 19*(6), 1873–1881. doi:10.1109/JBHI.2015.2461555.

Patterson, M. E., Williams, D. R. (2002). *Collecting and analyzing qualitative data: hermeneutic principles, methods and case examples* (Vol. 9). Advances in Tourism Application Series. Champaign, IL: Sagamore Publishing, Inc. http://www.treesearch.fs.fed.us/pubs/29421.

Pellegrino, Edmund D (2002). 'Professionalism, Profession and the Virtues of the Good Physician'. *The Mount Sinai Journal of Medicine, 69*(6), 378–384.

Pellegrino, E. D., Thomasma, D. C. (1993). *The Virtues in Medical Practice*. New York: Oxford University Press.

Peppet, S. R. (2014). Regulating the internet of things: First steps toward managing discrimination, privacy, security and consent. *Texas Law Review, 93*, 85.

Percival, J., & Hanson, J. (2006). Big brother or brave new world? Telecare and its implications for older people's independence and social inclusion. *Critical Social Policy, 26*, 888–909. doi:10.1177/0261018306068480.

Petryna, A., Lakoff, A., Kleinman, A. (2006). *Global pharmaceuticals: Ethics, markets, practices*. Durham, NC: Duke University Press.

Population Reference Bureau. (2012). Fact sheet: World population trends 2012. http://www.prb.org/Publications/Datasheets/2012/world-population-data-sheet/fact-sheet-world-population.aspx.

Rashid, U., Schmidtke, H., & Woo, N. (2007). Managing disclosure of personal health information in smart home healthcare. In Vol. 4555 LNCS. *4th International Conference on Universal Access in Human-Computer Interaction, UAHCI 2007*. Beijing. http://www.scopus.com/inward/record.url?eid=2-s2.0-38149103634&partnerID=40&md5=6e8a9a957ac835d8d2ce6949be2b3a71.

Remmers, H. (2010). Environments for ageing, assistive technology and self-determination: ethical perspectives. *Informatics for Health and Social Care, 35*, 200–210. doi:10.3109/17538157.2010.528649.

Richards, N. M., King, J. H. (2013). Three paradoxes of big data. *Stanford Law Review Online, 66*, 41.

Rigby, M. (2007). Applying emergent ubiquitous technologies in health: The need to respond to new challenges of opportunity, expectation, and responsibility. *International Journal of Medical Informatics, 76*, S349–S352. doi:10.1016/j.ijmedinf.2007.03.002.

Robinson, L., Hutchings, D., Corner, L., Finch, T., Hughes, J., Brittain, K., & Bond, J. (2007). Balancing rights and risks: Conflicting perspectives in the management of wandering in dementia. *Health, Risk and Society, 9*, 389–406. doi:10.1080/13698570701612774.

Roush, C. V., Cox, J. E. (2000). The meaning of home: How It shapes the practice of home and hospice care. *Home Healthcare Nurse'* http://journals.lww.com/homehealthcarenurseonline/Fulltext/2000/06000/The_Meaning_of_Home__How_It_Shapes_the_Practice_of.15.aspx.

Sajid, A., Abbas, H. (2016). Data privacy in cloud-assisted healthcare systems: state of the art and future challenges. *Journal of Medical Systems, 40*(6), 155. doi:10.1007/s10916-016-0509-2.

Salathé, M., Bengtsson, L., Bodnar, T. J., Brewer, D. D., Brownstein, J. S., Buckee, C., et al. (2012). Digital epidemiology. *PLoS Computational Biology, 8*(7), e1002616. doi:10.1371/journal.pcbi.1002616.

Salih, R. M., Othmane, L. B., & Lilien, L. (2011). Privacy protection in pervasive healthcare monitoring systems with active bundles. In 311–315. *9th IEEE International Symposium on Parallel and Distributed Processing with Applications Workshops, ISPAW 2011–2011, ICASE 2011, SGH 2011, GSDP 2011*. Busan. http://www.scopus.com/inward/record.url?eid=2-s2.0-80051985951&partnerID=40&md5=313835fb53e08a59bd7ac0c0fc297dd8.

Schmidt, S., Verweij, B. (2013). The PHM-ethics methodology. In *Interdisciplinary Assessment of Personal Health Monitoring, 13–20. Studies in Health Technology and Informatics 187*. Amsterdam: IOS Press.

Srinivasan, V., Stankovic, J., & Whitehouse, K. (2008). Protecting your daily in-home activity information from a wireless snooping attack. In 202–211. *10th International Conference on Ubiquitous Computing, UbiComp 2008*. Seoul. http://www.scopus.com/inward/record.url?eid=2-s2.0-59249104484&partnerID=40&md5=1e281ed890df7c05a3a8635431665534.

Steele, R., Lo, A., Secombe, C., & Wong, Y. K. (2009). Elderly persons' perception and acceptance of using wireless sensor networks to assist healthcare. *International Journal of Medical Informatics, 78*, 788–801.

Stowe, S., & Harding, S. (2010). Telecare, telehealth and telemedicine. *European Geriatric Medicine, 1*, 193–197. doi:10.1016/j.eurger.2010.04.002.

Stuart, E., Moh, M., & Moh T. S. (2008). Privacy and security in biomedical applications of wireless sensor networks. In *Applied Sciences on Biomedical and Communication Technologies, 2008. ISABEL'08. First International Symposium on IEEE*, (pp. 1–5).

Stutzki, R., Weber, M. Reiter-Theil, S. (2013). Finding their voices again: A media project offers a floor for vulnerable patients, clients and the socially deprived. *Medicine, Health Care and Philosophy, 16*(4), 739–750. doi:10.1007/s11019-013-9468-2.

Subramaniam, C., Ravi, A., Nayak, A., & Thunuguntla, S. (2010). Actor based domain specific privacy model for U-healthcare system. In 381–385. *6th International Conference on Digital Content, Multimedia Technology and Its Applications, IDC2010*. Seoul. http://www.scopus.com/inward/record.url?eid=2-s2.0-77958029155&partnerID=40&md5=09d269edcb98a5d863e1069adb159f71.

Taddeo, M. (2010a). Trust in technology: a distinctive and a problematic relation. *Knowledge, Technology & Policy, 23*(3), 283–286.

Taddeo M. (2010b). Modelling Trust in artificial agents, a first step toward the analysis of e-trust. *Minds and Machines, 20*(2), 243–257. doi:10.1007/s11023-010-9201-3.

Taddeo, M. (2016). Data philanthropy and the design of the infraethics for information societies. *Philosophical Transactions of the Royal Society A, 374*(2083), 20160113. doi:10.1098/rsta.2016.0113.

Taddeo, M., Floridi, L. (2011). The case for E-trust. *Ethics and Information Technology, 13*(1), 1–3.

Tene, O., Polonetsky, J. (2013). Big data for all: Privacy and user control in the age of analytics. *Northwestern Journal of Technology & Intellectual Property*. http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/nwteintp11&section=20.

Tentori, M., Favela, J., González, V. M. (2006). Quality of privacy (QoP) for the design of ubiquitous healthcare applications. *Journal of Universal Computer Science, 12*(3), 252–269.

The NIH HMP Working Group, Peterson, J., Garges, S., Giovanni, M., McInnes, P., Wang, L., et al. (2009). The NIH human microbiome project. *Genome Research, 19*(12), 2317–2323. doi:10.1101/gr.096651.109.

Tiwari, P., Warren, J., Day, K. J., & McDonald, B. (2010). Some non-technology implications for wider application of robots assisting older people. *Health Care and Informatics Review Online* 14. http://www.scopus.com/inward/record.url?eid=2-s2.0-77954871749&partnerID=40&md5=3557bb5e0d8464c12be74e104ddc0e79.

Townsend, D., Knoefel, F., & Goubran, R. (2011). Privacy versus Autonomy: A Tradeoff Model for Smart Home Monitoring Technologies. In *Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS* (pp. 4749–4752).

United Nations. (2008). World population prospects—The 2008 revision'. Department of Economic and Social Affairs—Population Division. http://www.un.org/esa/population/publications/wpp2008/wpp2008_highlights.pdf.

van De Garde-Perik, E., Markopoulos, P., & De Ruyter, B. 2006. On the relative importance of privacy guidelines for ambient health care. In 189:377–380. *NordiCHI 2006: 4th Nordic Conference on Human-Computer Interaction—Changing Roles*. Oslo. http://www.scopus.com/inward/record.url?eid=2-s2.0-34547236121&partnerID=40&md5=4062eeeeda1e81c5a8d4adf5c45da72.

van Hoof, J., De Kort, H.S.M., Markopoulos, P., & Soede, M. (2007). Ambient intelligence, ethics and privacy. *Gerontechnology, 6*(3). doi:10.4017/gt.2007.06.03.005.00.

van Hoof, J., Kort, H. S. M., Rutten, P. G. S., & Duijnstee, M. S. H. (2011). Ageing-in-place with the use of ambient intelligence technology: Perspectives of older users. *International Journal of Medical Informatics, 80*, 310–331.

Wachter, S. (2017). *Privacy: Primus inter pares—privacy as a precondition for self-development, personal fulfilment and the free enjoyment of fundamental human rights'. SSRN Scholarly Paper ID 2903514*. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=2903514.

Wachter, S., Mittelstadt, B., Floridi, L. (2017a). Why a right to explanation of automated decision-making does not exist in the general data protection regulation. *International Data Privacy Law*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469.

Wachter, S., Mittelstadt, B., Floridi, L. (2017b). Transparent, explainable, and accountable AI for robotics. *Science Robotics, 2*, eaan6080.

Wang, Kai, Yan Sui, Xukai Zou, Durresi, A., & Shiaofen Fang. 2008. 'Pervasive *and trustworthy healthcare'*. In *Advanced Information Networking and Applications—Workshops, 2008. AINAW 2008. 22nd International Conference on IEEE*, (pp. 750–755). doi:10.1109/WAINA.2008.147.

Watson, R. W. G., Kay, E. W. & Smith, D. (2010). 'Integrating biobanks: Addressing the practical and ethical issues to deliver a valuable tool for cancer research'. *Nature Reviews Cancer, 10*(9), 646–651. doi:10.1038/nrc2913.

Wilkowska, W., Gaul, S., & Ziefle, M. 2010. A small but significant difference—the role of gender on acceptance of medical assistive technologies. In Vol. 6389 LNCS. *6th Symposium of the Workgroup Human-Computer Interaction and Usability Engineering, USAB 2010*. Klagenfurt. http://www.scopus.com/inward/record.url?eid=2-s2.0-78649935702&partnerID=40&md5=9b824c5ddfd552b4593e346417ff411f.

Wu, Y. H., Fassert, C., Rigaud, A. S. (2012). Designing robots for the elderly: Appearance issue and beyond. *Archives of Gerontology and Geriatrics, 54*, 121–126. doi:10.1016/j.archger.2011.02.003.

Yuan, W., Guan, D., Lee, S., & Lee, Y. K. (2007). The role of trust in ubiquitous healthcare. In, 312–315. http://www.scopus.com/inward/record.url?eid=2-s2.0-34748858124&partnerID=40&md5=07bdb12a37bc100b17efe7bd20f70713.

Ziefle, M., Röcker, C., & Holzinger, A. (2011). Medical technology in smart homes: Exploring the user's perspective on privacy, intimacy and trust. In 410–415. http://www.scopus.com/inward/record.url?eid=2-s2.0-80054976685&partnerID=40&md5=6f08c26340ba83a66f048771302be6eb.

Zwijsen, S. A., Niemeijer, A. R., & Hertogh, C. M. (2011). Ethics of using assistive technology in the care for community-dwelling elderly people: An overview of the literature. *Aging and Mental Health, 15*, 419–427. doi:10.1080/13607863.2010.543662.